INTELLIGENCE OVERSIGHT: IMPROVEMENT THROUGH CONTINUAL EVALUATION

by
Michael B. Homburg

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August, 2015

ABSTRACT

Recent intelligence disclosures, as well as, the perceived increase in media leak prosecutions have brought the topic of intelligence oversight to the center of the debate on government spying. This thesis identifies the importance of oversight, but also illustrates the dilemma of congressional dysfunction. The research presented provides a basis for future discussions of oversight and legislative action regarding intelligence laws and authorities.

Peter Gill's theory which ties intelligence oversight to the inherent public distrust of governments of democratic nations forms the foundation of the first chapter. The chapter expands upon Gill's assertions and attempts to correlate historic public trust levels with the authorities of the intelligence oversight bodies of United States, Canada, Great Britain, and Australia.

The second chapter provides an updated look at the research conducted by Dr. Amy Zegart on the effectiveness of congressional oversight of the IC. Previously, Zegart graded the effectiveness of congressional oversight using public source data from 1985 – 2005. This chapter conducts an updated analysis using public source data from 99th Congress to present.

Prosecuting those accused of leaking classified information to the media has always caused a contentious debate. From the government's standpoint, the purpose of criminal prosecution is to punish the offender and deter would be criminals. The third chapter tests classical deterrence theory by evaluating the deterrent effect of prosecuting leakers on would be whistleblowers. The results of this chapter overwhelmingly

illustrate the likelihood of prosecution is remote, and the characteristics of the cases do not meet the criteria for creating a deterrent effect.

This lack of deterrent effect combined with the negative perceptions of prosecuting leakers should be the impetus for Congress to introduce legislation targeting those individuals with unlawfully disclosing classified information. Based on the importance of intelligence oversight, the ineffectiveness of HPSCI and SSCI illustrated in the second chapter is particularly concerning. Absent structural reforms, this portfolio demonstrates the effectiveness of USIC oversight can be improved by merely enhancing committee staff capabilities through increases in numbers and reducing staff turnover.

Thesis Advisors: Sarah Broesamle Clark, Dr. Mark Stout, Dr. Leila G. Austin, Dr. Kathryn Wagner Hill

Acknowledgements

I would like to thank my wife, Jessica, for putting up with my seemingly unending procrastination, and Teddy for providing the motivation to finish.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

The term Democratic Dilemma represents the constant balancing between actions taken to ensure nation's security and the founding principles of liberty in democratic nations. As history has shown, this balancing act is more aptly described as a pendulum that swings towards more government power in times of insecurity, and more towards liberty as citizens feel more secure. The unauthorized disclosures of classified information by Edward Snowden appear to have fomented the swinging of the pendulum back towards liberty. In light of this potential shift, this essay examines the correlation of public trust and government oversight and the effectiveness of current USIC oversight.

Each chapter in this portfolio explores a different facet of intelligence oversight. The first chapter uniquely expands on Peter Gill's theory alleging intelligence oversight in democratic governments can be attributed to an inherent to public distrust of the government. Chapter two provides a fresh and updated comparative analysis between the work of the intelligence oversight committees and the congressional oversight committees. Chapter three explores the deterrent effect of prosecuting individuals accused of disclosing classified information to the media without authorization.

Chapter One, "TESTING THE LIMITS OF THE DEMOCRATIC DILEMMA," explores the theory proposed by Peter Gill that oversight and accountability in democracies can be tied to public distrust of government associated with democracies. This chapter uniquely expands on Gill's assertions by conducting a comparison of historic public trust levels with the powers of the intelligence oversight bodies of United

States, Canada, Great Britain, and Australia. The countries were chosen based on their status as four of the mature, economically advanced, and western democratic nations.

Chapter Two, "INTELLIGENCE OVERSIGHT: UP-GRADING EFFECTIVENESS," provides an update to the work of Dr. Amy Zegart on the effectiveness of congressional oversight of the IC. The foundation of this chapter is the perception of dysfunctional oversight of the IC has resulted in massive violations of our privacy, as well as the use of an outdated law to prosecute those that release classified information without authorization. Although it is easy to label congressional oversight as dysfunctional with relation to these two instances, it is important to grade its overall effectiveness against the baseline of activity for a wide range of congressional oversight committees. Previously, Zegart graded the effectiveness of congressional oversight using public source data from 1985 – 2005 (at five year intervals) whereas this chapter relied on data from the 99th Congress to present.

Chapter Three, "THE NON-DETERRENT EFFECT OF PROSECUTING LEAKS," presents issues related to the prosecution of individual(s) for the unauthorized disclosure of classified information to reporters based on interpretations of the Espionage Act of 1917. This chapter focuses on deterrent effect of using this statute to prosecute seven individuals between 1983 and 2013. This chapter focuses on the deterrent effect of using the statute to prosecute seven individuals between 1983 and 2015. The lack of convictions during this time period clearly illustrates a lack of deterrent effect, which is often at odds with the public outcry that the use of this law produces a chilling effect on potential sources and journalists. The results of this chapter illustrate the effects of a lack of reform by oversight authorities on one issue related to intelligence.

In order to understand intelligence oversight, it is important to define intelligence, as well as understand the importance of oversight in the associated form of government. Intelligence is most aptly described as "mainly secret activities- targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities."[1] As this definition suggests, intelligence has differing purposes depending on the actor and different structures based on the political system.

Intelligence agencies serve under the executive branch and collect prioritized information, which supports the development and execution of US policy. Intelligence is collected from varying types of sources and can simplistically be separated into intelligence collected through human sources (HUMINT) and intelligence collected through technical or signals intelligence (SIGINT). If done legally, these types of collection platform can provide information that is vital to our national security. If done through an abuse of government powers, intelligence collection can violate of our nation's founding principles: civil liberties.

The autonomy of security and intelligence services refers to their ability to operate in the absence of oversight of their actions by another agency, commission or political body. Peter Gill argues the level of autonomy of these services directly correlates to the political system of the country.[2] Thus, authoritarian regimes possess

[1] Peter Gill, "Theories of intellligence: Where are we, where should we go and how might we proceed?" In *Intelligence Theory: Key questions and debates*, by Peter Gill, Stephen Marrin and Mark Phythian, 208-223. (New York: Routledge , 2009): 214.

[2]Peter Gill, *Policing Politics: Security Intelligence in the Liberal Democratic State.(*New York: Frank Cass & Co. LTD, 1994):64-70.

security and intelligence agencies with little or no oversight, and democratic nations would have stringent oversight.

Democratic governments include nation-states where the people are governed by a representative body that is freely elected by the eligible population. Typically, mature democratic governments tend to be strong states. The stability of democratic governments allows these nation-states to focus on the security of the governed and thus focus intelligence and security agencies on the external threats to the constituency. While there are varying degrees of vulnerability in democratic nations to foreign 'attacks,' most democratic states focus their intelligence on protecting the nation's security and promoting economic prosperity.[3]

The inherent distrust of the government by the inhabitants of democracies results in oversight of the government's bureaucracies. Although secrecy is a necessary condition of the intelligence services' work, intelligence in a liberal democratic state needs to work within the context of the rule of law, checks and balances, and clear lines of responsibility. Democratic accountability, therefore, identifies the propriety and determines the efficacy of the services under these parameters. With regard to intelligence where the nature of the system is "mainly secret" one might expect would expect extensive oversight of the organizations.

Although Gill's oversight assertion hold true when comparing differing forms of government, this portfolio attempted to prove his assertions based on national levels of public trust in government. As previously stated, this portfolio reviewed national public

[3] Generalization formed from mission of Australia, Canada, United Kingdom, France, Germany intelligence agencies identified on their official websites (http://www.asio.gov.au/, http://www.verfassungsschutz.de/en/index_en.html, http://www.interieur.gouv.fr/, http://www.csis-scrs.gc.ca/index-eng.asp, and https://www.mi5.gov.uk/

trust polls and intelligence oversight authorities of United States, Canada, Great Britain, and Australia. The countries were chosen based on their status as four of the mature, economically advanced, and western democratic nations. My research concluded the United States possesses the most stringent intelligence oversight apparatus of the countries reviewed. As a result of the research, I unable to verify Gill's assertions held true for similar countries. This conclusion could have been limited by the lack of historical and consistently collected international public trust polling.

From the creation of the United States intelligence system by the National Security Act of 1947, oversight responsibilities were relegated to the congressional sub-committees first 30 years of its existence.[4] The first reforms of the intelligence apparatus took 30 years to implement and were in response to the investigation by the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, commonly referred to as the Church Committee, which revealed egregious civil and human rights violations where the FBI and CIA investigated individuals or groups based on their speech.[5] The Church Committee identified the FBI's program, referred to as the FBI's Counterintelligence Program (COINTELPRO), aimed at infiltrating and investigating categories of groups and individuals believed to threaten domestic peace including the Communist Party of the USA; Socialist Workers Party; the White Hate Group; the Black Nationalist-Hate Group and the New Left. In addition, the

[4] "A Look Back…The National Security Act of 1947, "Central Intelligence Agency, accessed May 1, 2015, https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/national-security-act-of-1947.html.
[5] Select Committee to Study Governmental Operations with Respect to Intelligence Activities. "Intelligence Activities and the Rights of Americans." April 23, 1976, accessed August 1, 2012, http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIb.htm.

Church Committee noted the FBI's use of intrusive and warrantless wire surveillance and the unlawful opening of the mail of U.S. persons.[6]

The findings of the Church Committee resulted in the establishment of two Congressional intelligence oversight committees, the United States Senate Select Committee on Intelligence (SSCI) and House Permanent Select Committee on Intelligence (HPSCI), in 1976 and 1977, respectively. In addition to the creation of legislative oversight bodies (HPSCI and SSCI), the Foreign Intelligence Surveillance Act of 1978 established the Foreign Intelligence Surveillance Court (FISC) to provide judicial oversight over the use of covert techniques to support national security investigations. Although judicial oversight provides an important piece of intelligence oversight, this portfolio focuses on the performance of the legislative oversight bodies.

HPSCI and SSCI hold public hearings on intelligence issues to advocate for the public debate, as well as hold closed-door sessions for classified portions of the same debate or other topics. The committees also have authority to investigate intelligence matters, which includes the power to compel witness testimony or document production through congressional subpoena. In addition, the committees have authority to legislate, which means they have the authority to confer with constituents, special interest groups, and the USIC to craft legislation that constrains, empowers, or reforms the bodies the committees oversee.

[6] Select Committee to Study Governmental Operations with Respect to Intelligence Activities. "Intelligence Activities and the Rights of Americans." April 23, 1976. http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIb.htm (accessed August 1, 2012).

Although considered to be the most effective tool in oversight, neither HPSCI nor SSCI, possess budgetary (or appropriations) authority over the intelligence community which they oversee. Members of each chamber's Appropriations Committee sit on each intelligence committee; however, budgetary authority over the USIC is delegated to the Appropriations Committee itself. The Appropriation's budget authority is limited to passage of an overall budget as opposed to allotting specific amounts for targeted programs which would defund untenable programs and force the intelligence agencies to focus resources on activities deemed important to Congress. HPSCI and SSCI may lack appropriation's authority; however, the committees have the authority to hold public and closed hearings, request briefings and conduct interviews, introduce and consider legislation; issue subpoenas for testimony, and authorize the use of funds appropriated to the USIC.

The inability to pass Intelligence Authorization legislation between FY 2006-2009, DOJ's use of the Espionage Act of 1917 to investigate and prosecute leakers, and the inability to pass intelligence reforms that could have potentially prevented the 9/11 attacks have all been cited as evidence of oversight failures. Rather than judging HPSCI and SSCI's oversight on one or two failures, this portfolio follows Zegart's method of comparing legislative activity levels (hearings held, legislation considered/passed, and legislative success rates) of HPSCI and SSCI to other House and Senate committees. Overwhelmingly, the comparison reveals that HPSCI and SSCI's level of legislative activity was less than the average of other committee activity levels.[7] Impartial

[7]Bryan Jones and Frank Baumgartner, "Policy Agendas Project: Datasets & Codebooks," Policy Agendas Project Web site, accessed May 1, 2015, http://www.policyagendas.org/page/datasets-codebooks.

evaluation of the numbers suggests that Congress has not spent enough time overseeing the USIC.

The common misperception of intelligence oversight is that it is solely meant to prevent intelligence failures and government abuses. However, oversight includes the drafting and consideration of laws under which the USIC operates. The unauthorized disclosure of classified information by Edward Snowden ignited a heated debate about government spying, oversight failures, and the prosecution of leakers. Oversight failure and the prosecution of leakers seem unrelated; however they are in fact intertwined. Once such statute, 18 U.S. Code § 793 - Gathering, transmitting or losing defense information, stands at the center of the debate about prosecuting leakers. The statute indicates the unauthorized disclosure of classified information to an unauthorized recipient is a crime punishable by up to ten years imprisonment, forfeiture of property and funds, and fines for each count.[8] Although this statute provides the justification for investigation media leaks, the identified leakers have sometimes been charged with or pled guilty to lesser charges.

Critics argue the use of statutes born out of the Espionage Act of 1917 is a draconian attempt to stifle first amendment rights and deter future whistleblowers. Moreover, critics argue the act was passed in response to foreign spy networks during World War I and should not be applied individuals releasing information to the media.[9] Supporters of media leak prosecutions point to the damage done to national security. In a speech delivered to the Heritage Foundation, Chairman of the House Select Committee

[8]Cornell Law School, "18 U.S. Code § 793 - Gathering, transmitting or losing defense information," Cornell Law School Web site, accessed May 1, 2015, https://www.law.cornell.edu/uscode/text/18/793.
[9]Charlie Savage, "For U.S. Inquiries on Leaks, a Difficult Road to Prosecution," New York Times, June 9, 2012, accessed March 28, 2015, http://www.nytimes.com/2012/06/10/us/for-us-inquiries-on-leaks-a-difficult-road-to-prosecution.html?_r=0.

on Intelligence, Representative Pete Hoekstra, clearly stated that "some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information."[10]

Journalists may not be liked, but no one is calling them spies regardless of the media spin. The unauthorized publication of classified information is received by a plethora of foreign intelligence agencies whereas spies typically provide information to a limited number of agencies. The damage caused by the compromise of either SIGINT or HUMINT is worth noting. A media report quoting or referring to HUMINT can result in the loss of access to the reporting channel either because of an overabundance of caution (often referred to as operational security) or in a worst case scenario the intelligence contained in the article is singular in nature and results in the imprisonment or execution of the source.

SIGINT compromises result in the loss of significant resources expended in the research, development and installation of the technology responsible for the collection platform. SIGINT collection is often facilitated by human sources; therefore, any compromise of a SIGINT platform could possible result in the imprisonment or death of a human source as described above. Some SIGINT platforms are designed for a particular target, but many SIGINT techniques are used for multiple targets. Thus, the compromise of either HUMINT or SIGINT to the media can have far reaching consequences.

[10]Pete Hoekstra, *Secrets and Leaks: The Costs and Consequences for National Security,* July 29, 2005, accessed August 8, 2011, http://www.heritage.org/research/reports/2005/07/secrets-and-leaks-the-costs-and-consequences-or-national-security.

As previously stated, critics of media leak prosecutions claim the draconian use of this outdated law deters potential whistleblowers. The purpose of criminal prosecution is two-fold: punish the offender and deter would-be criminals. Based on this perceived agreement on this point (albeit for different reasons), this portfolio reviewed the case particulars for historical prosecutions of media leaks to determine if they serve as a deterrent. The results overwhelmingly suggest that prosecuting media leaks do not serve as a deterrent to would be criminals. Critics of media leak prosecutions have claimed potential leakers would be deterred long before the disclosures of Bradley Manning and Snowden. Their disclosures, which are considered the most massive in history, along with the data presented in this chapter confirm the lack of deterrent effect. The lack of a deterrent effect combined with the negative perception of using 18 U.S. Code § 793 to prosecute media leaks should serve as an impetus for congressional consideration and potential introduction of legislation.

CHAPTER ONE: *TESTING THE LIMITS OF THE DEMOCRATIC DILEMMA*

INTRODUCTION

Almost all nations, regardless of size and economic condition, have found it necessary to develop a clandestine system for the purpose of gathering and analyzing information involving threats to the nation's security.[11] According to Mark Lowenthal, "each nation practices intelligence in ways that are specific-if not peculiar- to that nation alone."[12] Lowenthal's observation of the distinctive nature of intelligence provides an opportunity for research into national intelligence organizations and their associated structures. Disclosures of intelligence activities and failures often result in enormous scrutiny of any nation's intelligence services. However, little public attention is ever paid to the oversight apparatus responsible for overseeing these agencies.

Out of the 194 countries currently recognized by the U.S. State Department, approximately 116 countries have some sort of intelligence and/or security agency.[13] However, only about 19 of the 116, or 11%, of these countries possess an external oversight apparatus responsible for some form of supervision of the agencies. The 19 countries include the following countries that possess some form of democratic or parliamentary government: Argentina, Australia, Belgium, Canada, Croatia, Germany,

[11]Arthur S. Hulnick and Joe Wippl, "FOREIGN INTELLIGENCE AND SECURITY SYSTEMS." *Boston University*. 2009. http://www.bu.edu/ir/files/2010/06/Syllabi_IR_578_Hulnick.pdf (accessed April 10, 2013).1

[12] Mark Lowenthal, *Intelligence From Secrets to Policy* (Washington, DC: CQ Press, 2009), 11.
[13] U.S. State Department. *A-Z List of Country and Other Area Pages.* 2013. http://www.state.gov/misc/list/index.htm (accessed April 10, 2013).

Israel, Italy, the Netherlands, New Zealand, Norway, Poland, Romania, Slovakia, South Africa, South Korea, the U.S. and Great Britain.[14]

With respect to security and intelligence services, autonomy can be associated with a lack of oversight of the services by another agency, commission or political body. According to Peter Gill, the level of autonomy of these services directly correlates to the political system of the country. In particular, Gill alleges that the protection of human rights associated with democracies results in higher levels of oversight, where as in totalitarian regimes the survival of the state trumps the concerns of tactics used by the intelligence and security services.[15] Scholarship on the collective authorities, resources, oversight, and the duties of intelligence agencies of particular nations have been lacking thus far and efforts to incorporate accountability and oversight into the theory intelligence have been non-existent to date.[16]

Thus, Gill's assertion that the public distrust in government inherent in democracies presents a unique opportunity for transnational comparison of the oversight apparatus of democratic nations. Based on Gill's assessment of levels of oversight, there should be a correlation between public trust figures and the level of oversight amongst nations. For example, higher levels of public distrust for the national government should be correlated with more extensive oversight of the intelligence apparatus and vice versa.

---

[14] Anthony Glees, Philip H.J. Davies, and John N.L. Morrison, The Open Side of Secrecy: Britain's Intelligence and Security Committee (London: The Social Affairs Unit, 2006), 15.

[15] Peter Gill, *Policing Politics: Security Intelligence in the Liberal Democratic State.(*New York: Frank Cass & Co. LTD, 1994),

[16] Peter Gill, "Theories of intellligence: Where are we, where should we go and how might we proceed?" In *Intelligence Theory: Key questions and debates*, by Peter Gill, Stephen Marrin and Mark Phythian, 208-223. (New York: Routledge , 2009): 222.

This chapter uniquely expands on Gill's oversight theory through comparison of historic public trust levels with the powers of the intelligence oversight bodies of the United States, Canada, Great Britain, and Australia to determine if there is a correlation. Comparative analysis of intra-national intelligence oversight mechanisms is limited by the pool of countries that employ these bodies. For this essay, the countries were chosen based on their status as four of the mature and economically advanced, western democratic nations as well as their involvement in United Kingdom – United States of America Agreement (UKUSA).

DEFINING GOOD OVERSIGHT

As previously stated, the purpose of this chapter is to determine if there is any discernible link between historical median public trust levels and the level of intelligence oversight in democratic nations. Based on assumptions made from Gill's research and literature, I hypothesize that the nations whose populations generally possess a greater distrust in government will be associated with governments that have implemented stringent oversight of their intelligence organizations. Testing of this hypothesis requires a brief introduction to intelligence followed by an in depth analysis of public trust polling and oversight. The knowledge gained from this review will provide the basis for the analysis of the public trust numbers and oversight authorities associated with the United States, Australia, Canada and the United Kingdom.

The foundation of any scholarship regarding the study of intelligence systems requires the term to be clearly defined. A generally accepted definition of intelligence has not been developed to date. Some scholars limit the definition of intelligence to include only secret information, while others believe it is a combination of open source

and secret information. Others include any and all actions taken to obtain and process the information in the definition of intelligence. For the purposes of this essay, Peter Gill's definition of intelligence seems the most appropriate. According to Gill, intelligence can be defined as "mainly secret activities- targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities."[17]

An actor's intelligence system is comprised of intelligence agencies focused on their piece of the country's intelligence process. Intelligence services are usually classified as foreign, domestic or unitary. Foreign intelligence services, such as the Central Intelligence Agency (CIA) in the U.S. or the Secret Intelligence Service (MI6) in the U.K., typically focus on threats from outside a nation's borders whereas domestic intelligence services, such as the Federal Bureau of Investigation (FBI) in the U.S. and the Secret Service (MI5) in the U.K., focus on threats from within borders. The Canadian Security and Intelligence Service (CSIS) is an example of a unitary service where the foreign and domestic efforts are combined in one agency.

As Gill's definition suggests, intelligence has differing purposes depending on the actor and different structures based on the political system. Democratic governments include nation-states where the people are governed by a representative body that is freely elected by the eligible population. Typically, mature democratic governments tend to be associated with strong states. The stability of democratic governments allows these nation-states to focus on the security of the governed and thus focus intelligence and

[17] Peter Gill, "Theories of intellligence: Where are we, where should we go and how might we proceed?" In *Intelligence Theory: Key questions and debates*, by Peter Gill, Stephen Marrin and Mark Phythian, 208-223. (New York: Routledge , 2009): 214.

security agencies on the external threats to the constituency. While there are varying degrees of vulnerability in democratic nations to foreign 'attacks', most democratic states focus their intelligence on protecting the nation's security and promoting economic prosperity.[18]

With respect to security and intelligence services, autonomy can be associated with a lack of oversight of the services by another agency, commission or political body. Gill argues the level of autonomy of these services directly correlates to the political system of the country.[19] The inherent distrust of the government by the inhabitants of democracies results in oversight of the government's bureaucracies. With regard to intelligence where the nature of the system is "mainly secret" one would expect extensive oversight of the organizations.

As indicated above, Australia, Canada, the U.K. and the U.S. are amongst the 19 countries that employ some level of oversight including political commission, legislative body and or judicial process[20] over their respective intelligence communities. Although there is an abundance of literature detailing how to improve oversight or reasons why the U.S. have not reformed its oversight, I have been unable to identify any credible scholarly work indicating that any level of oversight can possibly prevent all intelligence

[18] Generalization formed from mission of Australia, Canada, United Kingdom, France, Germany intelligence agencies identified on their official websites (http://www.asio.gov.au/, http://www.verfassungsschutz.de/en/index_en.html, http://www.interieur.gouv.fr/, http://www.csis-scrs.gc.ca/index-eng.asp, and https://www.mi5.gov.uk/

[19] Peter Gill, *Policing Politics: Security Intelligence in the Liberal Democratic State.(*New York: Frank Cass & Co. LTD, 1994), 66-72.

[20] Generalization formed from information identified on Australia, Canada, United Kingdom, France, Germany intelligence agencies' official websites (http://www.asio.gov.au/, http://www.verfassungsschutz.de/en/index_en.html, http://www.interieur.gouv.fr/, http://www.csis-scrs.gc.ca/index-eng.asp, and https://www.mi5.gov.uk/. Knowledge of US intelligence oversight is based on eight years experience.

failures or abuses nor ensure that the agency(ies) it oversees will function 100% effectively or efficiently. However, the appropriate level of oversight can mitigate the potential for abuse and failure, vigorously investigate allegations of either and promote systematic changes based on lessons learned to minimize the chance of recurrence.

The majority of literature on the subject of intelligence oversight is American centric. In fact, research of the topic of intelligence oversight identified *The Open Side of Secrecy*, which details the first ten years of the United Kingdom's Intelligence and Security Committee, as one of the only scholarly works analyzing the effectiveness of oversight bodies or other issues related to oversight in countries other than the U.S. The absence of literature outside of the American-centric works could be problematic for this essay depending on the applicability of this research to foreign oversight apparatus. The lack of research regarding the topic could possibly be associated with a lack of scholarly interest, a lack of notable oversight or a lack of oversight records in other countries.

According to Amy Zegart, effective oversight is difficult to define. She attributes this difficulty to three things: 1) differing opinions of good oversight 2) conflicting mandates within agencies and 3) invisible and/or unaccountable oversight activities.[21] Zegart's analysis of the difficulties in analyzing oversight is spot-on. Government oversight could mean entirely different things to civil rights groups or supporters of open-government than it does intelligence officers or even judges. In addition, it is impossible to know or even estimate the number of or effect of every ad hoc briefing or communication with the oversight apparatus that occurs outside the normal course of

[21]Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 17-19.

business. Thus, evaluation of oversight is limited to the publically available information. As our analysis is limited by the publically available information, we must evaluate the founding authorities of the oversight mechanisms and the effectiveness.

Mathew D. McCubbins and Thomas Schwartz aptly compare the available means of conducting oversight to that of "police-patrol" or "fire alarm." In the "police-patrol" method, the oversight apparatus constantly reviews the body it oversees, much like a police-man patrolling the streets, whereas with the "fire-alarm" method is can be associated with intense oversight in response to a crisis or failure much like a firemen responding to a fire-alarm.[22] The framework and models used by McCubbins and Schwartz has become the foundation of significant research in the topic of intelligence oversight by researchers such as Loch K. Johnson and Zegart.

Johnson and Zegart have used the "police-patrol" and "fire-alarm" metaphors in their scholarly worked aimed at identifying the shortcomings of congressional oversight, reasons for congress' resistance to change and to support their recommendations for congressional oversight reform. Although both forms of oversight have their benefits, "police-patrol" is the most effective means of oversight when combined with budgetary and authoritative powers over the agencies. "Fire-alarm" is considered the most time efficient for congress where a considerable amount of their time must be dedicated the other issues (domestic and constituent) that aid in their re-election to office.[23]

[22]Mathew D. McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols and Fire Alarms," *American Journal of Political Science* (1984): 165-168.

[23]David Mayhew, *The Electoral Connection,* (New Haven: Yale University Press, 1974), 5-7.

In her book, *Eyes on Spies: Congress and the United States Intelligence Community*, Zegart provides comparative analysis of various Congressional oversight committees using data regarding committee meetings, legislation considered and legislation passed and committee experience. The evidence overwhelmingly suggests that Congressional intelligence oversight can be described as sporadic and inconsistent "patrolling" that reverts to the "fire-alarm" model after failures.[24]

In "Secret Spy Agencies and a Shock Theory of Accountability," Johnson describes what he terms as the "Shock Theory of Accountability." Johnson continues to use the metaphors coined by McCubbins and Schwartz, but differs slightly from Zegart's previous work on Congressional oversight. Johnson's analysis of intelligence accountability illustrates how recent intelligence failure or scandals have resulted in intense periods of oversight "patrolling" and remedial legislation aimed at preventing future lapses. Johnson coins the term, "Shock Theory of Accountability," to describe the "shock" of major intelligence failure or scandal and the resulting ripple effects of these events on oversight.[25]

As clearly indicated above, good oversight is difficult to identify and is subjective to the person describing it. The mere existence of oversight is a positive sign, especially when it comes to "mainly secret" activities in democratic states. Robust oversight is necessary to mitigate the chances of intelligence failures or scandals, but it also threatens

---

[24]Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 67-69.
[25]Loch K Johnson, "Secret Spy Agencies and a Shock Theory of Accountability." *The University of Georgia School of Public and International Affairs, accessed April 14, 2013, 1,* http://intl.uga.edu/Johnson%20occasional%20paper.pdf.

the "secrecy" in which intelligence is based. Research into the appropriate level of oversight is not the focus of this essay. As previously indicated, this essay will attempt to correlate public trust levels to the levels of intelligence oversight in democratic nations.

With the issues of intelligence and oversight presented, it is important to discuss the role of public trust in government. Research by Todd Donovan, David Denemark and Shaun Bowler attempted to reconcile dissimilar levels of public trust with 29 economically advanced democracies based on data from the 2004 ISSP module. The scholars noted a disparity in public trust amongst the democratic governments ranging from 9% in Japan to 55% in Denmark. In particular, they noted that only 31% of American's trust that people in the government will do what is right most of the time. This level of trust may seem low; however, the US ranks higher than 18 of the countries surveyed. Great Britain was close behind the U.S. with 29%, while Australians and Canadians indicated a higher level of trust in their governments with 40% and 37%, respectively.[26]

Donovan, et al set out to investigate the role of history and culture in public trust.[27] The group found that the economic conditions, anxieties about security and/or terrorism, and polarizing views of the contemporary views of the current political party all affect the levels of trust in government across nations differently and thus make

[26] Todd Donovan, David Denemark, and Shaun Bowler, "Trust in Government: The United States in Comparative Perspective." *Western Washington University*, accessed March 20, 2013, http://faculty.wwu.edu/donovat/trust.pdf.

[27]Todd Donovan, David Denemark, and Shaun Bowler, "Trust in Government: The United States in Comparative Perspective." *Western Washington University*, accessed March 20, 2013, http://faculty.wwu.edu/donovat/trust.pdf.

predictions difficult. The findings clearly show that irregular public trust numbers without data regarding the current state of national affairs prevents proper analysis. In addition, the group does not address the mitigating or aggravating effects of the evolution in news media over the last forty years. Undoubtedly, the advent of the 24-hour news cycle has had some effect on public trust levels. Although it is important to acknowledge the potential impact of the media on public trust, this issue is one for future study.

The work by Donovan, et.al aids in the investigation of oversight in democratic nations by identifying the pitfalls of trying to tie public trust to similar governments.[28] In some case, the sporadic collection of data circa events observed by the public to be successes or failures tends to skew the data to one extreme or the other. For example, Gallup.com polling data from 2002 indicated an 18% jump in favorable rating from 2000 polling. More than likely, the higher level of trust can be associated with the U.S. government action to bring those seen as responsible for the 9/11 attacks to justice. Polling data from 2005 indicates a 23% decline in the government's favorable rating from 2002 levels.[29] Most likely, this decline can be associated with the well-publicized reports indicating that intelligence failures that led the U.S. to war in Iraq in 2003.

THEORY AND HYPOTHESIS

Although a wealth of information can be found regarding comparisons national intelligence systems and their effectiveness, little comparative attention has been paid to

[28] Polling data can be skewed and/or limited by 1) the number of willing participants 2) the participants ability to understand the questions 3) the polls ability to provide available responses that can accurately depict the sentiment of the polled and 4) the ability of the polling organization to "randomly" select potential participants that accurately reflect the country's ethnic, religious and political consistency. Polling is not without merits; it provides a "general" idea of public sentiment regarding a particular issue.

[29] Gallup. *Gallup* . http://www.gallup.com/poll/5392/trust-government.aspx (accessed February 1, 2013).

oversight studies. In particular, scholars of oversight have focused on the American system and have limited these studies to the bureaucratic structure, effectiveness of the system and Congress's resistance to reform. Comparative analysis of intelligence oversight bodies can be just as useful for the policymakers as comparative analysis of the intelligence systems. This chapter attempts to determine what, if any, correlation can be made between public trust levels and the level of intelligence oversight in democratic governments. Inferences from Gill's assertions regarding oversight lead me to believe that the nation(s) that trust its government the least possesses the greatest level of oversight.

METHODOLOGY

The case studies for this chapter test the proposition that levels of intelligence oversight in democratic nations can be tied to the level of public trust. As previously stated, higher levels of public trust in government should be associated with a lesser degree of oversight of a nation's intelligence apparatus. The case studies will specifically look at the intelligence and oversight mechanisms of four of the five countries involved in the UKUSA agreement: United States, Australia, Canada and Great Britain. Historical public trust polling will be compared to the oversight mechanism for each nation to determine whether the level of public trust can be correlated to the level of oversight. For the purposes of this essay, the median level available public trust numbers are useful and sufficient for identifying a potentially cultural trust in the government by Australians, Canadians, Americans and Britons.

Glees, et al described intelligence oversight bodies in democracies as the external accountability mechanisms whose mission is two-fold: 1) to ensure efficient and effective operation of the agencies it oversees 2) to prevent abuses and violations of law.[30] Based on Gill's assertions one can expect some level of intelligence oversight in democratic governments. Even the slightest form of oversight can have some effect in accomplishing the mission. However, the most extensive oversight includes bodies that have some level of budgetary and/or administration authority over the agencies they oversee combined with intelligence experience of the oversight members.

The "police-patrol" and "fire alarm" oversight methods each offer positive accountability of intelligence agency activities. However, "police-patrol" provides a much more effective means based on the ability to prevent failures or crisis before they occur. As this means is more effective, this essay will assign a score of "1" for countries that employ "police-patrol" methods, a score of "0.5" for countries using the "fire alarm" method and a score of "0.75" for any country employing sporadic patrol. In addition, each nation will be assigned a score of "1" for the oversight organisms that possess either budgetary or other authority over the intelligence community of each nation. Countries with external oversight bodies that possess no authority over their intelligence structure will be assigned a score of "0.0" and countries with limited authority will be assigned a score of "0.5." Finally, a score of "1.0" will be assigned for countries that possess significant intelligence experience amongst personnel assigned to the particular nation's oversight bodies and a score of "0.5" for countries with little experience or regular turnover.

[30]Anthony Glees, Philip H.J. Davies, and John N.L. Morrison, The Open Side of Secrecy: Britain's Intelligence and Security Committee (London: The Social Affairs Unit, 2006), 13.

The overall oversight score, which combines a weighted score for both effectiveness and authority, will be assigned by the sum of the two scores for each country. If the hypothesis for this essay is correct, the countries associated with the lower public trust levels should be associated with the higher oversight scores. If the lower public trust numbers cannot be associated with the countries with higher levels of oversight, then the hypothesis is incorrect. Regardless of the outcome, the findings should produce a basis for future research.

MAIN DISCUSSION

The United Kingdom of Great Britain and Northern Ireland or the United Kingdom as it is often referred as, is notionally a Constitutional monarchy. In reality, the government is divided into an executive branch led by the Prime Minister and a bicameral legislative branch consisting of the House of Lords and the House of Commons. Unlike the United States, the United Kingdom does not have a constitution that clearly defines the rights of its citizens or other governing principals. The United Kingdom is governed through statutes and partly common law and practice. The country is broken down into 27 counties, 32 London boroughs and 1 City of London or Greater London, 36 metropolitan districts, and 56 unitary authorities.[31]

Britain's executive branch, the Cabinet, is not bridled by the checks and balances inherent in the U.S. system and thus enjoys supremacy beyond the U.S. President. The Cabinet may make appointments and declarations without conferring with the Parliament, where it enjoys the majority within the House of Commons. In addition, Great Britain

[31]" Background Note: United Kingdom," U.S. Department of State, Last Modified March 22, 2012, accessed July 29, 2012, http://www.state.gov/r/pa/ei/bgn/3846.htm.

does not possess a written Bill of Rights that protects specific civil rights. Only recently (1998), did Great Britain pass the Human Rights Act which offered individual and political liberties.[32]

The United Kingdom intelligence collection efforts are split amongst three national intelligence agencies. The Secret Intelligence Service, or MI6, is responsible for the Nation's collection of intelligence against foreign security threats. The General Communications Headquarters, or GHGQ, is responsible for the nations Signals Intelligence (SIGINT) and information security for the government and armed forces. The Secret Service, or MI5 as the agency is also known, is tasked with domestic counterintelligence and security responsibilities. Although fundamental differences between the British and American intelligence communities exist, MI6 is comparable to the CIA, GCHQ is similar to the National Security Agency, and MI5 is most like the FBI.[33]

The Intelligence Services Act of 1994 (ISA) established the Intelligence and Security Committee (ISC), which consists of representatives from the House of Lords and House of Commons. The Prime Minister appoints members to the ISC in coordination and with the concurrence of the opposition party. The members of the committee often change upon the election of a new majority party. The committee is tasked with financial, administration and policy oversight of the United Kingdom's three intelligence agencies and its powers are is limited to the supervision and evaluation of the

[32]Mark M. Lowenthal, *Intelligence From Secrets to Policy* (Washington, DC: CQ Press, 2009), .315.

[33]Todd Masse, "Domestic Intelligence in the United Kingdom: The Applicability of the MI-5 Model to the United States." *Congressional Research Service*, May 19, 2003: 4.

agencies' performance in regards to these matters.[34] The ISC reports its findings and recommendations to the Prime Minister before they are presented to Parliament.

Between 2007 and 2012, the ISC held approximately 23 formal meetings and 12 informal meetings a year in furtherance of its oversight duties and responsibilities.[35] As required in its founding legislation, the ISC produces an annual report regarding its yearly work, as well as special 'ad hoc' reports on issues deemed appropriate. Since its establishment in 1994 the ISC has complied with this requirement and produced 17 annual reports, as well as 10 special reports detailing the findings of the ISC's investigation into such events as 2002 terror attack in Bali, the 2005 terror attacks in London and the issue of Iraq's weapons of mass destruction program to name a few. [36]

Based on the publically available information, the work of the ISC can be described as both "police-patrol" and "fire-alarm." By holding 35 formal and informal meetings annually, the ISC has clearly demonstrated that the committee is fully engaged in its founding directive and is thus "patrolling" the bodies it oversees. The 10 'ad hoc' reports published since its founding suggests that the committee increases oversight in response to perceived intelligence failures and abuses by the United Kingdom's intelligence service. Unfortunately, by limiting the ISC's authority to supervision and evaluation of the intelligence services, the United Kingdom has limited the committee's ability to force change amongst the services or direct the services to allocate resources to

[34]Anthony Glees, Philip H.J. Davies, and John N.L. Morrison, The Open Side of Secrecy: Britain's Intelligence and Security Committee (London: The Social Affairs Unit, 2006), 173.
[35]The Intelligence and Security Committee. *Annual Reports.* http://isc.independent.gov.uk/committee-reports/annual-reports (accessed May 1, 2013).

[36] The Intelligence and Security Committee. *Annual Reports.* http://isc.independent.gov.uk/committee-reports/annual-reports (accessed May 1, 2013).

issues deemed important to Parliament. Based on the information provided, the United Kingdom's Total Oversight Score is as follows:

1.0 (police-patrol) + 0.0 (oversight with no authority) + 0.25 (limited experience) = 1.25

Australia's intelligence collection efforts are split between two national intelligence agencies and several agencies within the Australian Department of Defence. Australia's national intelligence services include the Australian Secret Intelligence Service (ASIS) and the Australian Security Intelligence Organisation (ASIO). ASIS is responsible for the collection of overseas foreign intelligence and is similar to the CIA, whereas ASIO is Australia's national security service and maintains a role similar to that of the FBI's counterintelligence mission. Similar to the FBI, the Australian Federal Police (AFP) serves as Australia's police force and is responsible for enforcement of federal laws. The AFP has grown its intelligence capabilities to meet ongoing security challenges; however, law enforcement remains its primary responsibility.[37]

The origins of Australia's intelligence oversight can be found in the Australian Security Intelligence Organisation Act 1979, which created the Parliamentary Joint Committee (PJC) to oversee ASIO. This committee was replaced in March 2002 by the Parliamentary Committee on ASIO, ASIS and DSD (PJCAAD). The PJC was replaced by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) based on the recommendations of the "Flood Report" in 2005.[38] The tension within Australia's parliamentary government resides between the political parties rather than between the

[37]Sally Neighbour, "Hidden Agendas: Our Intelligence Services." *The Monthly*, November 2010.

[38]Parliament of Australia. *House of Representatives Committees.* http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/role.htm (accessed May 1, 2013).

branches of government as is the case with the United States. To alleviate the inherent distrust between political parties, PJCIS consists of members appointed by the prime minister in consultation with the opposition party. Thus, the make-up of the committee often changes with the election of a new majority political party.

Although the committee was renamed in 2005, its oversight authorities are based on the Intelligence Services Act of 2001 (ISA). The act requires the PJCIS to review the administration and expenditures associated with Australia's intelligence community annually, investigate any matter referred to the committee by one of the Ministers and provide Parliament with an annual report of the committee's activities. Language contained in the ISA prevents the committee from unilaterally initiating investigations into intelligence matters and limits the information the committee can request and/or receive in furtherance of its oversight activities.[39] On its website, the PJCIS acknowledges its oversight abilities by stating that the language contained within the ISA limits the committee's "capacity to inquire into operational matters and the intelligence gathering and assessment priorities of the relevant intelligence agencies."[40]

Between 2007 and 2012, the PJCIS issued annual reports of its findings to the Prime Minister, as required by ISA. During this time period, the committee has also published approximately four reports a year based on reviews requested by Ministers (as required by law). In addition to the research and inspections necessary to conduct its

[39] Parliament of Australia. *House of Representatives Committees.* http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/role.htm (accessed May 1, 2013).

[40] Parliament of Australia. *House of Representatives Committees.* http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/role.htm (accessed May 1, 2013).

mandated oversight, the committee also received approximately six private briefings annually to aid in their efforts.[41] The information available does not the specific information discussed in the briefings or the committee attendance rate at these briefings. Thus, it is difficult to gauge their value towards the committees overall oversight.

As previously described, the PJCIS must conduct regular reviews of the administration and expenditures of the Australian intelligence community. The lack of budgetary authority, as well as the statutory limits placed on the committee's investigative efforts, prevents the committee from effectively overseeing the governed. Thus, Australia's Total Oversight Score is as follows:

0.75 (sporadic patrol) + 0.0 (oversight with no authority) + 0.25 (limited experience) = 1.0

Like the United Kingdom and Australia, Canada has a constitutional monarchy but is governed by a parliamentary democracy. The executive branch is headed by the Prime Minister and the Federal Ministry, which typically consists of officials from Parliament who are appointed by the Prime Minister. The legislative branch of the Canadian government consists of a bicameral Parliament including the Senate and House of Commons. The judicial branch includes the Supreme Court of Canada and a system of lower federal courts.[42]

---

[41] Parliament of Australia. *House of Representatives Committees.* http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/role.htm (accessed May 1, 2013).

[42]"*North America :: Canada,"* The Central Intelligence, 2012, accessed August 1, 2012, https://www.cia.gov/library/publications/the-world-factbook/geos/ca.html.

Unlike other democratic nations described in this essay, the Canadian approach to national security is issue based rather than based on the geographic location of the threat. As such, Canada's intelligence community includes agencies that other countries might not consider intelligence related. Canada's intelligence community includes the Canadian Security Intelligence Service (CSIS), the Communication Security Establishment Canada (CSEC), Canada Border Service Agency (CBSA), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canadian Air Transport Security Authority (CATSA), and the Privy Council Office (PVO).[43] CSEC is responsible for Canada's SIGINT, as well as information assurance missions and is similar to the NSA. CSIS represents Canada's intelligence collection agency and includes both foreign and domestic intelligence missions.

Prior to 1984, the Royal Canadian Mounted Police (RCMP) was responsible for both Canada's intelligence collection and national law enforcement efforts. In response to terrorist and espionage threats of the 1960s and 1970s, the RCMP was designated as the national police force and CSIS was created as the nation's national security agency. As the nation's security agency, CSIS is tasked with pro-actively identifying threats, analyzing information and producing intelligence products to inform and protect the government and its citizens from nation's threats which are currently prioritized as "terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure."[44]

[43]"Role of CSIS," Canadian Security Intelligence Service, 2012, accessed August 1, 2012, http://www.csis-scrs.gc.ca/bts/rlfcss-eng.asp.

[44]"Role of CSIS," Canadian Security Intelligence Service, 2012, accessed August 1, 2012, http://www.csis-scrs.gc.ca/bts/rlfcss-eng.asp

The CSIS Act not only created the agency itself, but also the oversight body for CSIS activities: the Security Intelligence Review Committee (SIRC). The Prime Minister appoints members to the SIRC in coordination and with the concurrence of the opposition party. The members of the committee often can change upon the election of a new majority party. The SIRC regularly reviews CSIS activities on behalf of Parliament and report their findings accordingly. The review of CSIS activities includes regular meetings with CSIS executives, visiting regional offices to understand daily operations, discussions with other security and intelligence personnel, as well as attendance at international intelligence forums,[45] and is based on a research plan approved by the committee.[46]

The oversight powers of the SIRC are so expansive that the bodies can review all of CSIS's holdings upon request and without the need for judicial or legislative warrant. However, the committee does not possess any legislative or budgetary authority over CSIS. As previously stated, the SIRC identifies potential flaws in CSIS practices and provides recommendations that address the issues. Since its founding in 1984, the SIRC has produce 28 annual reports[47] approximately 100 other special reports[48] detailing the committee's findings and recommendations on a variety of other issues.

The oversight mechanism in Canada is reflective of the parliamentary system. Oversight in Canada is founded in the distrust between the major parties, whereas U.S. oversight is founded in the inherent distrust between the executive and legislative branches of government. Although

[45]Security and Intelligence Review Committee. "Annual Reports." *Security and Intelligence Review Committee.* October 23, 2012. http://www.sirc-csars.gc.ca/pdfs/ar_2011-2012-eng.pdf (accessed May 1, 2013).

[46]Ibid.
[47]Ibid.
[48]Ibid.

the committee has extensive powers to review CSIS activities and records, it does not have any powers to curtail CSIS actions. Based on the provided description, intelligence oversight in Canada can be described as "police-patrol." However, this patrolling is limited by the committee's lack of legislative or budgetary authority over CSIS. Thus, Canada's Total Oversight Score is as follows:

.75 (sporadic patrol) + 0.0 (oversight with no authority) + 0.25 (limited experience) = 1.0

Unlike the previously reviewed countries, the United States is a constitution-based federal republic consisting of 50 states and one district. The federal government is divided into three branches: executive, judicial and legislative. The executive branch is headed by the President of the United States and his cabinet of appointed officials. The judicial branch consists of the Supreme Court and a lower system of federal courts. The legislative branch consists of a bicameral Congress including the House of Representatives and the Senate.[49] The United States government provides a unique system of checks and balances that ensures no branch of the government becomes too strong and ensures the nation's laws do not infringe on the rights of its citizens.

The United States Intelligence Community (USIC) consists of 16 federal agencies of federal government responsible for the collection of foreign and domestic intelligence in support of the national security and foreign policy strategies. The significant number of agencies within the USIC makes comparison with lesser resourced nations difficult and somewhat outside the purview of this essay. However, as previously discussed the CIA is responsible for the collection of foreign intelligence, the NSA is responsible for

[49]"North America :: United States," The Central Intelligence Agency, last modified, 2012, accessed August 1, 2012, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html.

the collection of SIGINT, and the FBI is responsible for domestic intelligence and counterintelligence.

The findings of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, commonly referred to as the Church Committee, revealed some of the most egregious violations of civil and human rights where the FBI and CIA investigated individuals or groups based on their speech and/or expressions.[50] Specifically, the Church Committee identified abuses by an FBI program, referred to as the FBI's Counterintelligence Program (COINTELPRO), aimed at illegally infiltrating and investigating groups believed to threaten domestic peace. In addition, the Church Committee noted the FBI's use of intrusive and warrantless wire surveillance and the unlawful opening of mail of U.S. persons.[51] The findings of the Church Committee resulted in the establishment of two Congressional intelligence oversight committees, the United States Senate Select Committee on Intelligence (SSCI) and House Permanent Select Committee on Intelligence (HPSCI), in 1976 and 1977, respectively.

Zegart dedicates a chapter of her book, Eyes on Spies: Congress and the United States Intelligence Community, on a comparative analysis between the activity of these oversight committees and the activity of other congressional committees between 1985 and 2005. The data presented clearly indicates a lack of activity by the committees,

[50] Select Committee to Study Governmental Operations with Respect to Intelligence Activities. "Intelligence Activities and the Rights of Americans." April 23, 1976, accessed August 1, 2012, http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIb.htm.

[51] Select Committee to Study Governmental Operations with Respect to Intelligence Activities. "Intelligence Activities and the Rights of Americans." April 23, 1976, accessed August 1, 2012, http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIb.htm.

especially when compared to committees associated with domestic responsibilities that can be associated with sporadic "patrolling" with occasional "fire-alarm" oversight. In addition, Zegart analyzes committee assignments over the identified years and identifies a high turnover rate combined with a lack of intelligence experience amongst committee personnel.[52]

Currently, neither committee, HPSCI nor SSCI, possess budgetary authority over the intelligence community. Members of each chamber's Appropriations Committee sit on each intelligence committee; however, budgetary authority over the committee is delegated to the Appropriations Committee itself. The Appropriation's budget authority is limited to passage of an overall budget as opposed to allotting specific amounts for targeted programs which would force the intelligence agencies to focus resources on activities deemed important to Congress.

Based on the information provided, the Total Oversight Score for the United States is as follows:

0.75 (sporadic patrol) + 0.5 (oversight with limited authority) + 0.25 (limited experience) = 1.5

Although historical U.S. public trust polling data can be easily found data back decades, consistently collected international polling data for public trust in government is not. Thus, determining an average public trust number for the countries is limited by the available data. The Edelman Trust Barometer provides the most consistent results for citizens of the United States, the United Kingdom, Canada, and Australia in response to the question, "How much do you trust the government to do what is right." Figure 1 illustrates the results of the Edelman Trust Barometer for 2008-2015.

[52]Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 55-84.

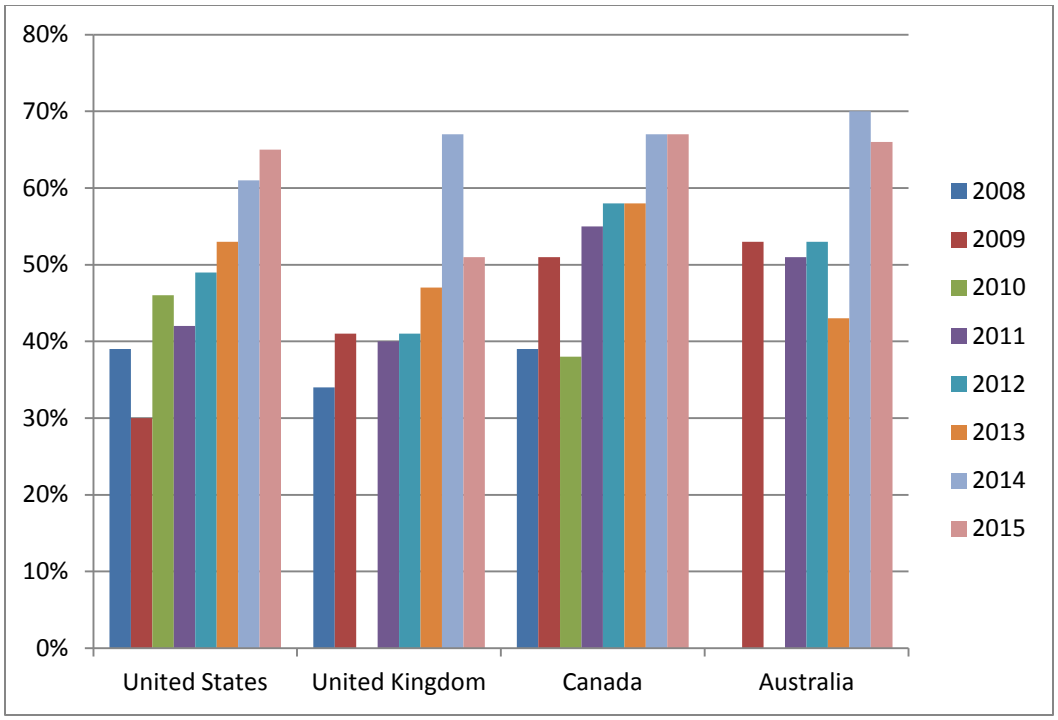

Figure 1: Edelman Trust Barameter 2008-2015 illustrating public trust in government to do what is right[53]

In order to mitigate the effects of natural fluctuations of public trust numbers, the average of the numbers from 2008-2015. Figure 2 illustrates the average public trust numbers for each country over this time period.

[53]"Edelman Trust Barometer Archive," Edelman Berland Website, 2015, accessed May 1, 2015, http://www.edelman.com/insights/intellectual-property/edelman-trust-barometer-archive/.

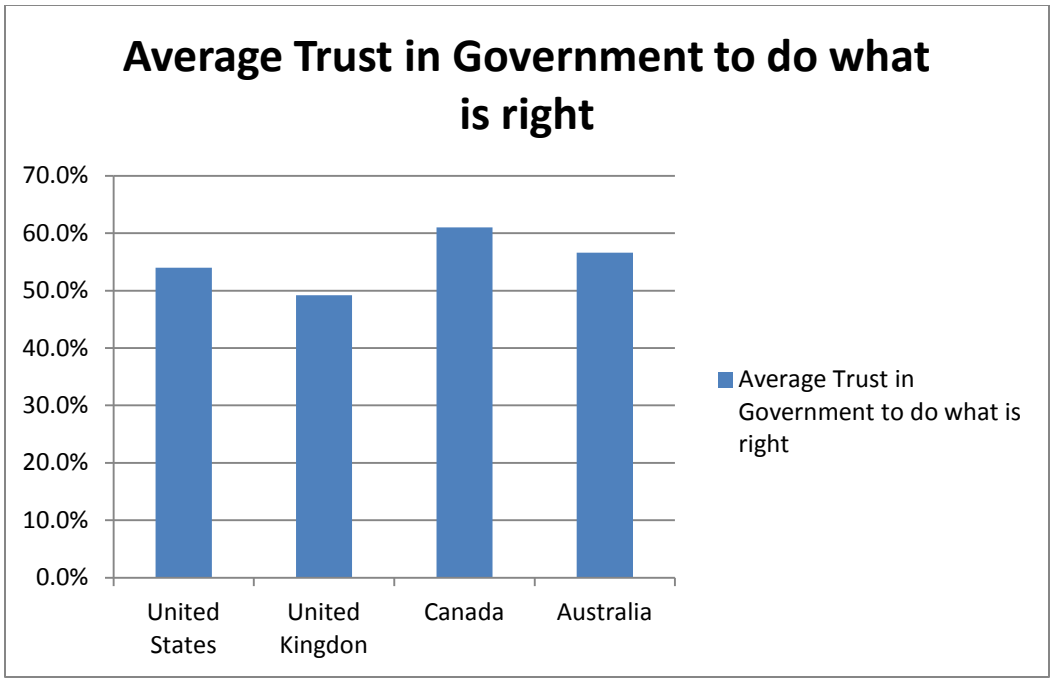

Figure 2: Average Trust in Government 2008-2015

RESULTS AND CONCLUSION

This review of the intelligence apparatus and oversight bodies of the United Kingdom, Australia, Canada and the United States reveals commonalities, as well as differences amongst the nations. As expected in democratic nations, the intelligence agencies have developed extensive and multi-layered oversight mechanisms including legislative review that sometimes requires the prior approval of activities, peer and judicial approval for implementation of intrusive techniques, and accountability to the executive branch governments in all of the countries.

If the hypothesis for this chapter were correct, the lowest levels of public trust would be associated with the greatest intelligence oversight. The United Kingdom (followed by the United States, Australia, and then Canada) would have the highest level of intelligence oversight based on their low levels of public trust. However, by looking at

the intelligence oversight by countries and associating a score based on the authorities granted to each oversight entity, a different picture can be seen. The following oversight scores clearly indicate that the United States possesses the most extensive oversight of the countries reviewed:

1) United States 1.5
2) United Kingdom 1.25
3) Canada and Australia (tied) 1.0

So what does it all mean? Clearly, the hypothesis for this essay was miscalculated or the methodology used for testing did not accurately reflect the oversight powers associated with each country. Another reason for the discrepancy could lie in the countries chosen for comparison. Comparison of intelligence services of between countries with democratic and authoritarian regimes would have likely been more appropriate. The choice of comparing similar western democratic governments might have resulted in public trust numbers that were too close for comparison, especially when considering potential margins of error with the data collection.

Public trust polling in the United States goes back decades whereas the polling for this chapter is limited to the 2008-2015 timeframe. The lack of comparable polling data (for the other countries reviewed) over more historic and consistent time period could have skewed the public trust numbers a couple of percentage points either way. Specifically, the polling data could have been unusually high or low in any of the countries due to isolated crisis or instances of national pride.

Future research of this topic should consider whether comparison should include the 116 countries with intelligence or security agencies or a larger subset of the 19

democratic countries. Using a larger sub-set of less similar and democratic countries might include wider variations public trust numbers which allow for more definitive conclusions. In addition, the larger country pool may provide enough data to allow for conclusions regarding the effect of changes in levels of oversight on the public trust polling numbers.

The accuracy of future research could be increased with the existence of regular and continuous polling, over an extended period of time that investigates the level of the public's trust in the effectiveness of the intelligence community, as well as the public's trust in the intelligence community's respect for civil liberties and the nation's laws. As discussed in the public trust literature, the results are only as good as the polling pool and the data input.

CHAPTER TWO *INTELLIGENCE OVERSIGHT: UP-GRADING EFFECTIVENESS*

INTRODUCTION

Prior to the Edward Snowden's release of classified information, the public debate surrounding the prosecution of individuals accused of disclosing classified information without authorization typically focused on issues involving the First Amendment, a citizens' right-to-know, over-classification of government information, deterrence, selective prosecution, and appropriate legal remedies. Snowden's disclosures about mass surveillance programs under broad authorities granted under section 215 of the Foreign Intelligence Surveillance Act (FISA) shocked the public and confirmed the suspicions of transparency and privacy rights' groups. Media outlets decried the perceived violation constitutional protections and questioned if USIC oversight had failed. [54] To answer that question, this chapter evaluated the effectiveness of USIC oversight effectiveness and presented recommendations for improvement.

In order to evaluate the performance of the intelligence oversight committees, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI), it is important to understand the authorities and available means to execute their authorities. The committees hold public hearings on intelligence issues to advocate for the public debate, as well as hold closed-door sessions for classified portions of the same debate or other topics. The committees also have authority to investigate intelligence matters, which includes the power to compel witness

[54]Ezra Klein, "Edward Snowden, Patriot," Washington Post, August 9, 2013, accessed March 1, 2015, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward-snowden-patriot/.

testimony or document production through congressional subpoena. In addition, the committees have authority to legislate, which means they have the authority to confer with constituents, special interest groups, and the USIC to craft legislation that constrains, empowers, or reforms the bodies the committees oversee.

Currently, neither committee, HPSCI or SSCI, possess budgetary authority over the intelligence community which they oversee. Members of each chamber's Appropriations Committee sit on each intelligence committee; however, budgetary authority over the USIC is delegated to the Appropriations Committee itself. The Appropriation's budget authority is limited to passage of an overall budget as opposed to allotting specific amounts for targeted programs which would defund untenable programs and force the intelligence agencies to focus resources on activities deemed important to Congress. Although HPSCI and SSCI lack budgetary authority, they have been entrusted with other powers that can be used to oversee the USIC.

So, how can we judge the effectiveness of congressional oversight? In her book, Zegart provides an innovative and comparative analysis of various Congressional oversight committees using data regarding committee meetings, legislation considered and legislation passed and committee experience. Zegart's analysis uses this data to determine if Congress is fulfilling the four roles of intelligence oversight: Policeman, Board of Directors, Coach and Ambassador.[55] Zegart's work overwhelmingly suggests that Congressional intelligence oversight can be described as sporadic and inconsistent with spikes in legislative activity in response to failures. Rather than judging HPSCI and SSCI's oversight of one or two programs disclosed by Snowden, this chapter follows

[55] Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 31.

Zegart's method of comparing legislative activity levels (hearings held, legislation considered/passed, and legislative success rates) of HPSCI and SSCI to other House and Senate committees.

Overwhelmingly, the comparison reveals that HPSCI and SSCI's level of legislative activity was less than the average of other committee activity levels.[56] Wishful thinking might lead one to hope the committees are executing their authorities with less activity, but realistically these percentages suggest that Congress has not spent enough time overseeing the USIC. In addition to confirming the need for increased USIC oversight, this chapter expanded on and updated Zegart's research, and provides recommendations for improving USIC oversight.

LITERATURE REVIEW

According to Jennifer Kibbe, government oversight of the USIC plays intelligence role is the most important based on the inability of the media to keep the government in check when it comes to intelligence. The mere existence of oversight is a positive sign, especially when it comes to "mainly secret" activities in democratic states. Robust oversight is necessary to mitigate the chances of intelligence failures or scandals, but it also threatens the "secrecy" in which intelligence is based. Good oversight is difficult to identify and is subjective to the person describing the mechanism.[57]

As previously stated, the most important reason for intelligence oversight is the inherent secrecy of the subject. In addition to overseeing the USIC, congressional

[56]Bryan Jones and Frank Baumgartner, "Policy Agendas Project: Datasets & Codebooks," Policy Agendas Project Web site, accessed May 1, 2015, http://www.policyagendas.org/page/datasets-codebooks.
[57] Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 18.

oversight committees also play an important in explaining and representing the USIC to the public, as well as improving the intelligence product.[58] Public (or open hearings) provide the most useful tool in educating the public about the work of federal agencies. The classified nature of intelligence presents a unique challenge for HPSCI and SSCI to hold substantive hearings aimed at educating the public about national security threats and/or USIC efforts to neutralize those threats. .

Between 1947 and 1975, over 200 bills aimed at reforming and/or increasing oversight of the USIC.[59] As evidenced by the number of bills and oversight literature, the examples of the ineptitude of intelligence oversight and opinions of how to improve oversight are abundant. Often cited as evidence of the committees' ineptitude include their inability to pass Intelligence Authorization legislation between FY 2006-2009, the DOJ's use of the Espionage Act of 1917 to investigate and prosecute leakers, and their inability to pass intelligence reforms that could have potentially prevented the 9/11 attacks.[60]

The most notable recommendations for improving intelligence oversight were included in the U.S. National Commission on Terrorist Attacks Upon the United States, commonly referred to as the 9/11 Commission. The commission recommended either consolidating appropriation and authorization authority in HPSCI and SSCI or the creation of a joint standing committee on intelligence modeled after the Joint Committee

[58]Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," Intelligence and National Security25:1 (2010):25, accessed May 1, 2015, doi:10.1080/02684521003588104.
[59]Harry Rowe Ransom, "Congress and the Intelligence Agencies," Proceedings of the Academy of Political Science 32:1 (1975), 162.
[60]Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," Intelligence and National Security25:1 (2010):26, accessed May 1, 2015, doi:10.1080/02684521003588104.

on Atomic Energy.[61] However, the current partisan environment hinders the introduction and passage of legislation aimed at reforming intelligence oversight. Partisanship and "turf wars" between the Appropriations Committees (which currently possess budgetary authority over the USIC) and HPSCI and SSCI have been cited as reasons congress has not reformed the current intelligence oversight structure.[62]

With all these opinions about USIC oversight, one might think someone might suggest there was a solution or combination of solutions that could prevent intelligence failures and abuses. Richard Betts argues intelligence failures are inevitable and describes thoughts to the contrary as illusory.[63] However, the appropriate level of oversight can mitigate the potential for abuse and failure, ensure the vigorous investigation allegations of both, and promote systematic changes based on lessons learned to minimize the chance of recurrence. The questions raised by the disclosures of Edward Snowden is whether the oversight committees have been effectively executing their authorities to ensure proper oversight and what, if anything, can be done to improve.

Although the recommendations for oversight reform have merit, the examples of congressional dysfunction that form the basis for these proposals are based on generalities. The basis for intelligence reform should be grounded in empirical evidence and proven models rather than opinions. According to Kibbe, "the most influential model on intelligence oversight divides oversight activity into two metaphorical

[61]Elaine L. Halchin and Frederick M. Kaiser, "Congressional Oversight of Intelligence: Current Structure and Alternatives," CSRS Report RL32525 (Washington: Congressional Research Service, 2012), 9.
[62]Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 121.
[63]Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failure is Inevitable?," *World Politics* 31 (1978):61.

categories: 'police patrols' and 'fire alarms.'"[64] The metaphors, coined by Mathew D. McCubbins and Thomas Schwartz, aptly compare the available means of conducting oversight to that of a policeman patrolling the streets or a firemen responding to a fire-alarm.[65] The framework and models used by McCubbins and Schwartz has become the foundation of significant research in the topic of intelligence oversight by researchers such as Loch K. Johnson and Zegart.

Johnson and Zegart have used the "police-patrol" and "fire-alarm" metaphors in their scholarly worked aimed at identifying the shortcomings of congressional oversight, reasons for congress' resistance to change and to support their recommendations for congressional oversight reform. The "police-patrol" model uses consistent oversight monitoring to detect, remedy and deter inappropriate behavior whereas the "fire-alarm" model relies on the media, interest groups, or whistleblowers to alert congress and the public of potential violations.[66] Although both forms of oversight have their benefits, "police-patrol" is the most effective means of oversight when combined with budgetary and authorization powers over the agencies. "Fire-alarm" is considered the most time efficient for Congress where a considerable amount of their time must be dedicated the other issues (domestic and constituent) that aid in their re-election to office.[67]

In "Secret Spy Agencies and a Shock Theory of Accountability," Johnson describes what he terms as the "Shock Theory of Accountability." Johnson continues to

---

[64]Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," Intelligence and National Security25:1 (2010):27, accessed May 1, 2015, doi:10.1080/02684521003588104.
[65]Mathew D. McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols and Fire Alarms," *American Journal of Political Science* (1984): 165-168..
[66] (Grossman and Simon 2008, 437)
[67]David Mayhew, *The Electoral Connection,* (New Haven: Yale University Press, 1974), 5-7.

use the metaphors coined by McCubbins and Schwartz, but differs slightly from Zegart's previous work on Congressional oversight. Johnson's analysis of intelligence accountability illustrates how recent intelligence failure or scandals have resulted in intense periods of oversight "patrolling" and remedial legislation aimed at preventing future lapses. Johnson coins the term, "Shock Theory of Accountability," to describe the "shock" of major intelligence failure or scandal and the resulting ripple effects of these events on oversight.[68]

Zegart dedicates a chapter of her book, *Eyes on Spies: Congress and the United States Intelligence Community*, to a comparative analysis between the activity of these oversight committees and the activity of other congressional committees between 1985 and 2005. The data presented clearly indicates a lack of activity by the committees, especially when compared to committees associated with domestic responsibilities. Zegart's work overwhelmingly suggests that Congressional intelligence oversight can be described as sporadic and inconsistent "patrolling" that reverts to the "fire-alarm" model after failures.[69]

After finding HPSCI and SSCI to be ineffectively executing their oversight authorities, Zegart attributes this ineffectiveness to a lack of Congressional and public interest. Zegart finds a lack of experience and a lack of tenure on the committees, and a lack of incentive of members to volunteer for these assignments due to the lack of electoral effect. Zegart concludes oversight expertise can be increased by tapping into

---

[68]Loch K Johnson, "Secret Spy Agencies and a Shock Theory of Accountability." *The University of Georgia School of Public and International Affairs, accessed April 14, 2013, 1,* http://intl.uga.edu/Johnson%20occasional%20paper.pdf.

[69]Amy B. Zegart, Eyes on Spies: Congress and the United States Intelligence Community (Stanford: Hoover Institution Press, 2011), 55-84.

the legislator's homegrown knowledge, altering rules to enhance on the job training (e.g. end HPSCI term limits and incentivize activity), and leverage congressional resources to enhance staff capability.[70] Zegart's suggestion that congressional oversight can be judged through committee meetings, legislation considered and legislation passed and committee experience provides an acceptable means to gauge committee effectiveness and served as the basis for the case studies in this chapter.

After illustrating the ineptitude of intelligence oversight, Zegart presents statistics related to public interest groups and spending on intelligence lobbying in an attempt to correlate congressional dysfunction to a lack of public interest. The statistics cited illustrate the lack of funds spent on intelligence lobbying (as a sub-set of defense lobbying), as well as a lack of Foreign Affairs interests groups. In addition, compares the committee member assignments and committee staffing levels of HPSCI and SSCI to other congressional committees. This comparison indicates less member experience and seniority for HPSCI and SSCI, as well as inadequate staffing levels. As a result of her research, Zegart recommends improving the intelligence oversight committees by consolidating budgetary authority within HPSCI and SSCI, incentivizing member service, eliminating HPSCI term limits, and increasing staff personnel and capabilities. [71]

Zegart's supporters cite her use of metrics (legislative activity, congressional staffing levels, lobbying dollars spent, etc.) to evaluate the effectiveness of the intelligence oversight committees in comparison to others committees and industries. William N. Nolte suggests these metrics provide empirical data which conclusively

[70]Amy B. Zegart, Eyes on Spies: Congress and the United States Intelligence Community (Stanford: Hoover Institution Press, 2011), 86-87.
[71]Amy B. Zegart, Eyes on Spies: Congress and the United States Intelligence Community (Stanford: Hoover Institution Press, 2011), 55-84.

illustrates an overall ineffectiveness of intelligence oversight, identifies potential causes of the performance, as well as potential solutions to be considered by Congress.[72] Zegart's unique approach presents statistic-based reform recommendations rather than recommendations based on anecdotal, interest-biased, or even after-action review panels such as the 9/11 Commission.

Critics of Zegart's methodology argue that the oversight effectiveness cannot be solely measured merely by the number of hearings or reports published.[73] More important than the number of hearings or reports, is what transpires in the hearings or meetings or the content of the reports. In addition to the hearings themselves, it is important to consider the congressional response hearings. For example, what does the committee do with the information provided or the knowledge gained? Does the committee request additional information (either written or through testimony)? These questions require an in depth analysis of oversight by issue rather than an evaluation of intelligence oversight as a whole. However, "quality oversight requires a minimum level of attention, and comparison to other congressional oversight interests gives an important indicator of institutional attention."[74]

Although support of Zegart's work include, Nolte notes that Zegart's conclusions may be limited by her choice of records (1985-2005) and should be updated to determine if her findings still hold true. Zegart's choice of a five-year sampling data between 1985

[72]William M. Nolte, "Measuring Congressional Dysfunction," International Journal of Intelligence and Counterintelligence (2013): 417-420, accessed May 1, 2015, doi:10.1080/08850607.2013.758009.
[73]Kenneth Anderson, October 17, 2011, book review of *Eyes on Spies: Congress and the United States Intelligence Community* by Amy B. Zegart, Lawfare Blog, October 17, 2011, http://new.lawfareblog.com/eyes-spies-amy-b-zegart.
[74]Kenneth Anderson, October 17, 2011, book review of *Eyes on Spies: Congress and the United States Intelligence Community* by Amy B. Zegart, Lawfare Blog, October 17, 2011, http://new.lawfareblog.com/eyes-spies-amy-b-zegart.

and 2005 limited her dataset to five data points (1985, 1990, 1995, 2000, and 2005). If Zegart's findings would have been based on data for each Congress, her findings would have been more substantive based on 10 likely data points. The recent disclosures by Snowden combined with the importance of intelligence oversight in our democracy, requires us to update and improve upon the small imperfections of Zegart's work.

THEORY AND HYPOTHESIS

As previously stated, the purpose of this chapter is to characterize the effectiveness of HPSCI and SSCI at conducting oversight of the USIC. In light of the disclosures by Snowden and based on the previous work by Zegart, I hypothesize that HPSCI and SSCI's sporadic execution of oversight authorities continue to make the committees less effective than other congressional oversight committees. The sporadic oversight can likely be tied to the relative unimportance of intelligence to the American public, which ultimately leads to neglect in Congress.

METHODOLOGY

Although intelligence oversight in the US is more stringent than in other western democratic governments, the lack of appropriations authority prevents the USIC oversight apparatus from wielding the most important tool necessary for effective oversight.[75] According to the literature reviewed for this essay and other sections of this portfolio, oversight structures can be graded on the strength of the body as defined by its founding authorities, as well as its effectiveness in executing its responsibilities using its authorities. Without budgetary authority, analyzing the four roles of Zegart's' model for

[75]Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," Intelligence and National Security25:1 (2010):29, accessed May 1, 2015, doi:10.1080/02684521003588104.

intelligence oversight (Policeman, Board of Directors, Coach, and Ambassador) provides the most effective means to grade the institutions of USIC oversight.[76] However, closed hearings and other limitations associated with classified information prevent an evaluation of each of these four roles in an unclassified setting.

Following McCubbins' theory that police patrolling type of oversight was the most effective means to practice oversight, this chapter conducted a baseline analysis and comparison of data and statistics of other Congressional Committees to the performance of the House and Senate Intelligence Committees (HPSCI and SSCI). The average committee performance served as a baseline of activity to be considered. Legislative activity about the average would be considered "police-patrolling" and lower levels would be considered less effective and more likely to follow the "fire alarm" model.

For the purposes of this chapter, committee performance was judged purely through a statistical comparison rather than focus on a specific topic covered by the committees. Committee activity was defined as the number of committee hearings held (regardless of type); legislative activity in terms of bills introduced and considered by each committee, as well as the number of those bills becoming laws; and number of committee reports issued. Although Zegart did not include committee reports in her work, they were included in this chapter to provide a more complete picture of committee activity because they are provide documentation of legislation measure reported for

[76]Amy B. Zegart, Eyes on Spies: Congress and the United States Intelligence Community (Stanford: Hoover Institution Press, 2011), 31.

chamber action, detail oversight and investigative activities, reports of conference committees, and other committee activity reports.[77]

As with Zegart's work, this chapter relied on publically available U.S. government information to identify a baseline for the average activity level for HPSCI and SSCI to other legislative committees possessing oversight responsibilities and detailed a comparison between the average of activity and activity by the House and Senate Intelligence Committees to rate their effectiveness of the committee.[78] This chapter gathered data from the 99th Congress to the 110th Congress as opposed to a five-year sampling (Dr. Zegart's method). The findings of this chapter validated Zegart's previous findings with minor qualifications and suggestions that will help refine future scholarly research on USIC oversight.

MAIN DISCUSSION

Zegart's originality in using legislative activity statistics to illustrate inept congressional oversight received well deserved praise. However, the use of five-year samplings over a twenty year time period raised questions of whether her findings would hold true over a longer period of time. As previously stated, this purpose of this chapter was to test Zegart's findings held true over the course of time and using more consistent metrics. As with Zegart, this chapter reviewed legislative activity (Number of Committee Hearings and Reports issued, to determine the overall effectiveness of HPSCI and SSCI (in comparison to other committees) and attempted to tie this effectiveness to a lack of attention in Congress.

[77]"All Legislation," Library of Congress Web site, accessed February 7, 2015, https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%7D.
[78] Due to the lack of publically available records documenting HPSCI hearings, the chapter did not conduct a comparison of House committee hearings.

Nolte correctly questioned whether Zegart's findings would hold true if a larger dataset were analyzed, but he fails to note her use of five or ten year samplings for a majority of her metrics. In Zegart's defense, she notes that her team reviewed her sampling to ensure events such as hearings related to the 9/11 attacks would not overinflate the numbers. However, Zegart fails to account for the possibility the statistics of other committees were biased by events and failures under the jurisdiction of those committees. The Veterans Affairs' scandal and the Affordable Care Act website rollout illustrate how oversight failures of other committees could inflate the responsible committees' statistics. In order to compensate for these anomalies, committee activities should be measured more consistently than a five-year sampling and over a greater period of time.

The data collected (illustrated in Table 1 and Table 2) clearly indicates that SSCI holds fewer hearings than other committees[79], and both HPSCI and SSCI issue fewer committee reports, introduce and consider less legislation, and ultimately have less legislation introduced (by the committees) become enacted laws as a by-product of introducing less legislation. Although SSCI held fewer hearings, the committee appeared to be quite active with numerous on-the-record and off-the-record briefings during each Congress. SSCI recorded 106 on-the-record briefings and interviews, as well as numerous off-the-record briefings in addition in addition to the 35 hearings held during

[79]A comparison of HPSCI hearings was not possible for an extended period of time due to the lack of publically available information.

the 109th Congress.[80] During the 106th Congress, SSCI recorded 17 on-the-record briefings and over 250 off-the-record briefings in addition to the 69 hearings held.[81]

[80]Senate Select Committee on Intelligence, "Report of the Select Committee on Intelligence, Covering the Period January 4, 2005 to December 8, 2006 - Senate Report 110-57," Senate Select Committee on Intelligence Web site, April 26, 2007, accessed May 1, 2015, http://www.intelligence.senate.gov/publications/report-select-committee-intelligence-covering-period-january-4-2005-december-8-2006.

[81]Senate Select Committee on Intelligence, "Committee Activities, Special Report of the Select Committee on Intelligence, January 6, 1999 to December 15, 2000 - Senate Report 107-51," Senate Select Committee on Intelligence Web site, August 30, 2001, accessed May 1, 2015. http://www.intelligence.senate.gov/publications/committee-activities-special-report-select-committee-intelligence-january-6-1999.

Congress	Average Number of Committee Hearings	Commerce, Science, and Transportation	Environment and Public Works	Finance	Foreign Relations	Homeland Security and Governmental Affairs	Health, Education, Labor and Pensions	SSCI
99th (1985 - 1986)	84	95	70	123	44	84	104	102
100th (1987 - 1988)	108	125	96	109	39	115	103	*
101st (1989 - 1990)	110	166	95	111	53	131	119	83
102nd (1991 - 1992)	111	127	77	109	84	138	153	81
103rd (1993 - 1994)	74	152	74	119	55	162	124	92
104th (1995 - 1996)	77	93	40	79	56	74	74	102
105th (1997 - 1998)	80	138	46	60	62	102	51	77
106th (1999 - 2000)	88	107	63	63	101	70	89	69
107th (2001 - 2002)	64	157	65	74	65	115	103	38
108th (2003 - 2004)	85	45	40	63	119	105	61	16
109th (2005 - 2006)	76	133	34	78	80	170	63	35
110th (2007-2008)	83	29	21	100	71	153	75	82
111th (2009 - 2010)	82	102	*	45	88	143	39	79
112th (2011 – 2012)	*	*	*	*	*	*	*	80
113th (2013 – 2014)	*	*	*	*	*	*	*	111

Table 1: Senate Select Committee on Intelligence Consistently Holds Fewer Hearings than Other House Committees, 99st Congress – 113 Congress.[82]

Although legislative activity statistics indicate HPSCI and SSCI are associated with lower levels of legislative activity, the legislative success rate for HPSCI and SSCI far exceeds that of other committees as well as the average success rate for each Congress. In fact, SSCI's legislation success rate is 125% of the committee average and HPSCI's legislation success rate

[82] Data: Policy Agenda Project was the source of all committee data except SSCI. Since the Policy Agenda Project is limited to data from published open hearings, SSCI hearing data was obtained from http://www.intelligence.senate.gov.pubactivities.html.

is 225% of the committee average. The effect of divided (or unified) government appears to have little effect on the average legislative success rates in congress. Although the average legislative success rate is slightly higher for periods of divided government as opposed to periods of unified government, periods of divided government experience both the highest and lowest legislative success rates. The effect of partisanship outside the scope of this essay and should be researched in future

Congress	Congressional Legislative Success Rate	HPSCI Legislative Success Rate	SSCI Legislative Success Rate	HSPCI Reports Issued	Percentage of Average Reports Issued by Other House Committees	SSCI Reports Issued	Percentage of Average Reports Issued by Other Senate Committees	Government
101st (1989-1990)	5.64%	5.88%	0%	6	*	5	*	DIVIDED
102nd (1991-1992)	5.08%	14.29%	17%	9	*	4	*	DIVIDED
103rd (1993-1994)	4.82%	25.00%	6%	3	*	2	*	DIVIDED
104th (1995-1996)	4.22%	25.00%	11%	6	14%	6	22%	UNIFIED
105th (1997-1998)	4.42%	6.25%	29%	6	22%	4	18%	DIVIDED
106th (1999-2000)	5.57%	27.27%	0%	4	16%	3	16%	DIVIDED
107th (2001-2002)	3.55%	23.81%	13%	2	8%	3	14%	DIVIDED
108th (2003-2004)	4.72%	5.88%	11%	5	16%	4	12%	UNIFIED
109th (2005-2006)	3.69%	9.09%	0%	6	27%	4	19%	UNIFIED
110th (2007-2008)	3.28%	6.82%	0%	4	18%	5	19%	DIVIDED
111th (2009-2010)	2.82%	2.17%	0%	****	12%	****	8%	UNIFIED
112th (2011-2012)	2.31%	16.67%	9%	****	49%	****	23%	DIVIDED
113th (2013-2014)	2.78%	1.61%	17%	****	27%	****	28%	DIVIDED

Table 2: Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence consistently exceed legislative success rates for each Congress.[83]

[83]"All Legislation," Library of Congress Web site, accessed February 7, 2015, https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%7D.

scholarly work on the legislative process.

Zegart illustrates a lack of public interest in intelligence through superficial analysis of interest groups and lobbying dollars spent by industry.[84] Although her conclusions regarding the public's interest are correct, her choice of limiting her analysis to these statistics is curious. With her first dataset, Zegart's compiled the list of organized and registered interest groups, and subjectively identified the ones she felt could likely be involved in intelligence as a means to quantify the number of foreign affairs interest groups. This process resulted in statistics indicating Foreign Affairs Interest Groups accounted for only 4.4% of the total number.[85]

Zegart correlates congressional inaction to a lack of public interest using statistics from public interest groups and money spent on lobbying. For public interest groups, Zegart cites examples of Sister Cities International and Gays and Lesbians in Foreign Affairs as "unlikely to be involved in intelligence."[86] A more in depth evaluation of each group's charter and review of the group's activities would be needed to solidify Zegart's conclusions. This subjective assessment disregards the circumstances where these associations could be involved with lobbying or public promotion of positions related to intelligence.

Similarly, Zegart relies on lobbying dollars spent by industry to support the lack of public interest argument. For her analysis, Zegart subjectively combined industries

[84]Amy B. Zegart, *Eyes on Spies: Congress and the United States Intelligence Community* (Stanford: Hoover Institution Press, 2011), 76.
[85]Ibid, 76
[86]Ibid, 76

identified in the statistics she cited from the Center for Responsive Politics to fit her narrative. This aggregation of industries muddles the facts behind the statistics. Specifically, Zegart extrapolates the Intelligence lobbying must only be a subset of the 5% of lobbying dollars spent on the Defense Industry. In this instance, it appears Zegart included Intelligence under the Defense Industry because almost its entire budget is hidden inside the Defense Budget.

Zegart's methodology of viewing intelligence-related lobbying as a subset of Defense spending does not account for the role of telecoms and other electronic communication carriers in intelligence collection. In response to the Snowden disclosures, *Yahoo* and *Facebook* executives revealed the companies complied with lawful requests for records or access to information but also fought against request the companies deemed unlawful. The executives also revealed classified legal process prevented the companies from being more transparent with their consumers.[87] Clearly, this scenario illustrates the potential for these types of companies to lobby congress on behalf of legislation involving data collection and retention, transparency, and privacy constituent rights. Further illustrating this point is the fact that Defense sector lobby ranked tenth of the measured sectors between 1998 and 2015, whereas the Communications/Electronics sector ranked fifth.[88] Thus, the amount of money spent lobbying on behalf of intelligence or intelligence related issues could be higher than assumed when viewed outside the realm of the Defense subset.

[87]Siobhan Gorman and Jennifer Valentino-DeVries, "New Details Show Broader NSA Surveillance Reach: Programs Cover 75% of Nation's Traffic, Can Snare Emails," Wall Street Journal, August 20, 2013, http://www.wsj.com/articles/SB10001424127887324108204579022874091732470.
[88] (Ranked Sectors n.d.)

This 'pre-Snowden' mentality disregards the public and non-public relationship companies or industries may have in the machinery of the USIC.[89] Although her conclusions regarding dollars spent on Intelligence lobbying is correct, an exhaustive analysis of where the lobbying dollars were spent would be necessary to confirm her assessment. This analysis would include a comparison of lobbying dollars and contact reports for specific intelligence related legislation, as well as an in depth analysis of each lobbying report filed for each Congressmen and Senator before, during and subsequent their assignment on one of the intelligence committees.

Unless Zegart acknowledged the limitations of these statistics, she could have offered additional data confirming a lack of public interest. Specifically, Zegart should have caveat the use of her data and then provided historical national election exit polling data to illustrate the absence of Intelligence or Government Oversight as a prominent voter issue. This date could have showed empirical evidence illustrating a potential reason for congressional inaction and/or lack of attention.

Zegart indicated congressional leaders did not spend as much time on intelligence oversight because the work on these committees took time away from constituent issues and thus hurt re-election campaigns. In essence, Congressman representing rural or industrial districts preferred to spend time on agricultural and trade issues which affected their constituent's everyday life. Based on the classified nature of most of the work on intelligence oversight, Congressmen are prevented from the type of credit-claiming that

[89]Siobhan Gorman and Jennifer Valentino-DeVries, "New Details Show Broader NSA Surveillance Reach: Programs Cover 75% of Nation's Traffic, Can Snare Emails," Wall Street Journal, August 20, 2013, http://www.wsj.com/articles/SB10001424127887324108204579022874091732470.

members of other committees can do to illustrate their work on behalf of their constituents.

National Election Year	Polling Organization	Most Important Issues for Voters
2014	NBC	Economy 44% Healthcare 25% Illegal Immigration 14% Foreign Policy 13%
2012	CNN	Economy 60% Healthcare 17% Federal Budget Deficit 17% Foreign Policy 4%
2010	CNN	Economy 52% Deficit 8% Healthcare 8% Illegal Immigration 8% Education 8%
2008	CNN	Economy 62% Iraq 10% Healthcare 9% Terrorism 9%
2006	CNN	Iraq 49% Terrorism 46% Economy 33% Illegal Immigration 29% Moral Issues 25%
2004	CNN	Moral Issues 22% Economy 20% Terrorism 19% Iraq 15% Healthcare 8%
2002	USA Today	Economy 25% Potential War in Iraq 25% Terrorism 14% Social Security/Medicare 11% Education 11% Healthcare 9%

Table 3: Most Important Issues in National Elections[90]

[90] Data: 2014 http://www.nbcnews.com/politics/elections/exit-polls-show-economy-tops-voters-concerns-n241426, , 2012 http://politicalticker.blogs.cnn.com/2012/11/06/exit-polls-top-issues-for-voters/, 2010

As evident from the historical national election exit polling in Table 3, the issues of intelligence, congressional performance, intelligence oversight, or privacy rights are never mentioned as any of the major voter issues. The polling data appears to indicate voters value issues they perceive to affect them directly such as the economy, which is affected by employment, immigration, health care, and other moral issues. However, careful review of the exit polls indicates the questionnaires for the polls actually provided choices for the 'most important issue" and none of the polls included choices for and indicates the polling methodology provided the respondents with the ability to choose issues of intelligence, congressional performance, intelligence oversight, or privacy rights.

Limiting the response choices for national exit polling questions forces the respondent's to decide which of the declared issues is the most important to them and may prevent additional relevant and/or fringe issues from being identified. Although this methodology potentially prevents intelligence related issues from being identified as most important issues, other polling suggests that intelligence or civil rights issues are not important in national elections. According to a recent Pew Survey, the public's lack of interest in intelligence oversight may also be attributed to an ignorance of who is

---

http://www.cnn.com/ELECTION/2010/the.issues/ 2008
http://www.cnn.com/2008/POLITICS/11/04/exit.polls/, 2006
http://www.cnn.com/ELECTION/2006/special/issues/ 2004
http://www.cnn.com/ELECTION/2004/pages/results/states/US/P/00/epolls.0.html, 2002
http://usatoday30.usatoday.com/educate/.../**2002**1030-**elections**.pdf

responsible.[91] This lack of interest or ignorance of the public regarding government programs is not surprising in light of comments made by Jonathan Gruber, key architect of the Affordable Care Act. Gruber admitted the law was passed by exploiting the ignorance of the American public.[92] One can only wonder how an uninformed public can hold Congress accountable for overseeing the USIC, which is an entity in which few people have experience with or knowledge of and even less feel any connection with. This sentiment rings true in light of Gruber's comments about healthcare, which is a topic that affects everyone directly.

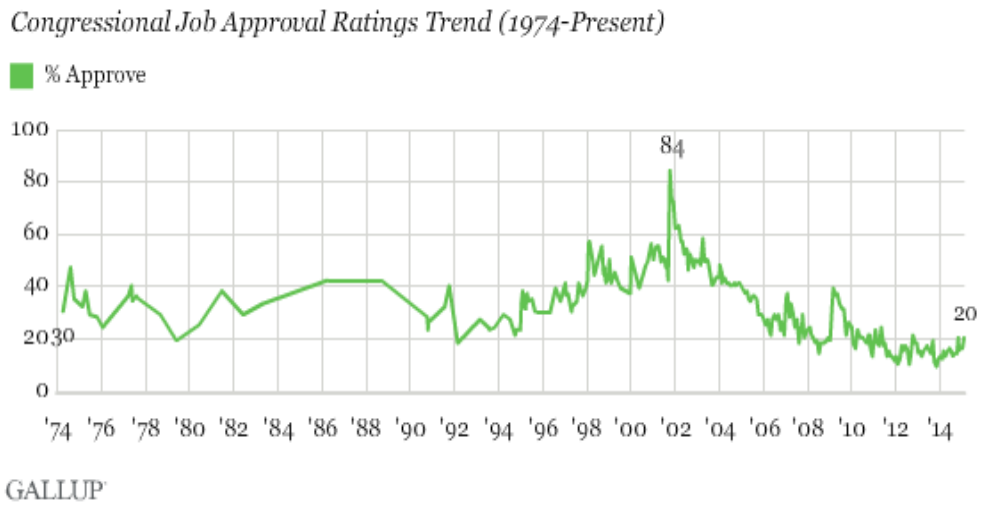

Figure 3: Congressional Job Approval Ratings Trend (1974-Present)[93]

[91]Lee Rainie and Mary Madden, "Americans' Privacy Strategies Post-Snowden," Pew Research Center Web site, March 16, 2015, accessed March 16, 2015, http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/.
[92]Ilya Somin, "Key architect of Obamacare admitted that it was passed by exploiting political ignorance," Washington Post, November 11, 2014, accessed May 1, 2015, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/key-architect-of-obamacare-admitted-that-it-was-passed-by-exploiting-political-ignorance/.
[93]Gallup, "Congress and the Public," Gallup Web Site, accessed March 13, 2015, http://www.gallup.com/poll/1600/congress-public.aspx.

Although Congressional job approval rating have plummeted since their historic highs in the wake of the 9/11 terror, the current disapproval ratings are associated with partisan politics, political gamesmanship, gridlock, and economic issues. None of the responses recorded by Pew attributed the respondent's disapproval of Congress to failures of intelligence oversight or intelligence matters. Moreover, overhauling the USIC or the USIC oversight structure, or even increasing privacy rights were not included in the top recommendations of those polled on how to fix Congress.[94]

In addition to legislative activity levels, Zegart attributed some of the congressional ineptitude to the size of the HPSCI or SSCI staffs. As evident from Table 4 below, HPSCI and SSCI staff size still lag behind those of the Banking and Armed Services committees. Although HPSCI and SSCI staffing levels have expanded and contracted over time, the current levels indicate an expansion between 1977 and 2014.

[94]Gallup, "Congress and the Public," Gallup Web Site, accessed March 13, 2015, http://www.gallup.com/poll/1600/congress-public.aspx.

House of Representatives Committee Staff Levels 1977 - 2014						
	1977	1987	1997	2007	2014	% Change 1977 -
Armed Services	40	61	55	53	66	65%
Banking	51	74	58	43	68	33%
Intelligence	23	17	24	39	32	39%
Senate Committee Staff Levels 1977 - 2014						
	1977	1987	1997	2007	2014	% Change 1977 -
Armed Services	32	54	59	51	49	53%
Banking	46	40	37	47	47	2%
Intelligence	40	38	30	34	41	3%

Table 4: House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence Consistently possess fewer professional staff members than other committees.

Although committee staffing levels certainly affect HPSCI and SSCI's ability to execute their duties, data collected by the Sunlight Foundation suggests high staff turnover rates compounds staffing issue at a minimum. As illustrated in Table 5 below, HPSCI is one of only three House committees possessing a retention rate of less than 40%. The Sunlight Foundation suggests that high turnover rate likely causes the committee to be less effective at executing their duties, and increasing reliant on lobbyists to help analyze and draft legislation.[95]

According to the Center for Responsive Politics, the number of registered lobbyists increased from 10,405 in 1998 to 11,781 in 2014 (11.7% increase), and dollars spent on lobbying increased from $1.45 Billion to $3.23 billion (122.8% increase) during the same time period. Over the same period and based on the number of clients, the top issues lobbied included Federal Budget/Appropriations, Health, Defense, Taxes, and

[95]Lee Drutman, February 6, 2012, "Turnover in the House: Who keeps – and who loses – the most staff," Sunlight Foundation Web site, accessed May 1, 2015, http://sunlightfoundation.com/blog/2012/02/06/turnover-in-the-house/.

Transportation. From 2005-2014, the bills receiving the most lobbying efforts involved Healthcare, Employment issues, Federal Budget/Appropriations, and Disaster Relief. None of these bills included Intelligence related matters.[96] If the Sunlight Foundation's assertion is correct, diminished staffing levels, high turnover rates amongst committee staffs, and a lack of intelligence related lobbying spending severely limit HPSCI and SSCI's ability to execute their authorities. Researchers with the Sunlight Foundation noted common themes amongst committees/members having lower staff turnover included higher salaries. In addition, senior members and democratic members were more likely to have higher retention rates than junior and/or republican members.[97]

Committee	Staff in 3rd quarter 2009	… who stayed through 3rd quarter 2011	Retention rate
Natural Resources	64	23	35.9%
Education & The Workforce	79	30	38.0%
Intelligence	36	14	38.9%
Oversight & Government Reform	108	44	40.7%
Transportation & Infrastructure	83	34	41.0%
Energy & Commerce	114	50	43.9%
Ethics	22	10	45.5%

[96]"Lobbying Database," Center for Responsive Politics Website, accessed May 1, 2015, http://www.opensecrets.org/lobby/.
[97]Lee Drutman, February 6, 2012, "Turnover in the House: Who keeps – and who loses – the most staff," Sunlight Foundation Web site, accessed May 1, 2015, http://sunlightfoundation.com/blog/2012/02/06/turnover-in-the-house/.

Financial Services	81	38	46.9%
Veterans' Affairs	34	16	47.1%
Science, Space & Technology	65	31	47.7%
Homeland Security	67	32	47.8%
Small Business	31	15	48.4%
House Administration	47	23	48.9%
Appropriations	226	112	49.6%
Foreign Affairs	81	41	50.6%
Armed Services	68	36	52.9%
Agriculture	49	26	53.1%
Rules	35	19	54.3%
Judiciary	84	46	54.8%
Ways And Means	79	44	55.7%
Budget	42	27	64.3%
Joint Committee On Taxation	68	56	82.4%

Table 5: House Permanent Select Committee on Intelligence rates amongst the highest staff turnover rates for Congressional committees.[98]

Zegart attributed the lack of incentives for high ranking members, or Movers and Shakers as she termed them, to seek HPSCI and SSCI assignments. For the period

[98]Lee Drutman, February 6, 2012, "Turnover in the House: Who keeps – and who loses – the most staff," Sunlight Foundation Web site, accessed May 1, 2015, http://sunlightfoundation.com/blog/2012/02/06/turnover-in-the-house/.

analyzed by Zegart (1977 – 2007), the number of Movers and Shakers declined. In the years since (2007-2015), the number has risen dramatically. Although the reason for the increase is unclear at this time, the possibilities include the natural fluctuation in numbers or an increased focus on USIC oversight predicated by the Snowden disclosures.

Committee	***Year***	***Movers and Shakers***	***Committee Size***	***% of Movers and Shakers***
SSCI	2015	13	19	68%
	2007	5	15	33%
	1997	9	19	47%
	1987	11	15	73%
	1977	6	17	35%
HPSCI	2015	6	21	29%
	2007	5	20	25%
	1997	7	16	44%
	1987	8	17	47%
	1977	6	13	46%

Table 6: The number of movers and shakers on the House Permanent Select Committee on Intelligence and Senate Select Committee have fluctuated over time.

Zegart also attributes committee assignment term limits as an issue that prevents members from gaining the necessary experience in intelligence matters to effectively execute their duties. The problem with this argument is that SSCI removed term limits years ago and HPSCI currently employs a term limit of four terms (8 years). If Zegart's assertion were true, how could the USG expect almost every other USIC agency to effectively execute its mission when the agency heads and executive leadership management retire or move on? There have been four Secretaries of Defense and six

CIA Directors, but yet those agencies continue to accomplish their mission. Why can these bureaucracies continue to function, but congressional oversight fails? The reason these agencies/departments have been able to continue functioning at a high level with this excessive turnover is likely due the professional staff under their command.

RESULTS AND CONCLUSION

Although intelligence failures are inevitable, oversight done correctly can mitigate the potential for abuse and failure. Zegart's analysis of the difficulties in analyzing oversight is spot-on. Government oversight could mean entirely different things to civil rights groups or supporters of open-government than it does intelligence officers or even judges. This chapter's expansion of Zegart's statistical analysis of intelligence oversight confirmed her previous findings indicating USIC oversight was less active, and thus less effective, than other congressional oversight committees. However, this essay provides additional data to support her findings as well as suggest additional research.

As the literature review illustrated, the most effective tool in oversight is budgetary authority. Until Congress drafts and approves legislation to consolidate budgetary authority with the intelligence committees, efforts must be made to improve oversight within the current framework. With the exception of unauthorized disclosures (and sometimes authorized) to the media, the classified nature of intelligence also precludes the media from being an effective tool in oversight.

As the research has shown, it is impossible to know or even estimate the number of every ad hoc meetings or briefings, or communications amongst the oversight apparatus that occurs outside the normal course of business[99] and thus, evaluating congressional oversight is limited to the publically available and documented information. Thus, HPSCI and SSCI must improve their focus on transparency to include increased public hearings, as well as increase the tracking and publication of committee activities associated with their oversight duties. Beyond holding the USIC accountable, transparency in oversight activities can help educate the public and spur public debate on intelligence which had been lacking before the Snowden disclosures.

Zegart's work tied the perceived lack of Congressional oversight to a variety of factors revolving around the relative unimportance of intelligence matters to national elections. As evidence, Zegart cited fewer dollars spent on lobbying Intelligence-related issues, less Intelligence interest groups, less movers and shakers on the committees, fewer incentives for committee members, and other matters as evidence of why committee members do not spend the appropriate time dedicated to their work on HPSCI and SSCI. This chapter's review of exit polling for historical national elections only confirms Zegart's assessment of the relative unimportance of Intelligence to voters, lobbyists, and congressional members seeking re-election.

Zegart's conclusions about the reasons for the lack of attention are correct; however, her assessment of the most effective means to remedy the situation should be refined. Zegart mentions increasing committee staff levels in her recommendations for

[99] As evidenced from the inability to gauge HPSCI's legislative activity levels.

improving oversight, but she considers committee member experience and attention to committee work to be more important. I disagree. Most of the oversight workload is handled by the committee staff. In order to improve the consistency and effectiveness of USIC oversight, Congress should focus on increasing committee staff levels and capabilities, as well as increasing staff retention rates for HPSCI and SSCI. As the Sunlight Foundation suggests, higher salaries or other monetary compensation provides the easiest means to increase and retain committee staff. However, this would only be a temporary solution since other committees would likely follow suit. Therefore, future research of intelligence oversight should focus on USIC committee staffing issues.

The public reporting of congressional legislative activity is slightly delayed and at times inconsistent, but the increase in SSCI hearings during the 113th Congress could be indicative of patterns associated with McCubbins description of Congressional Intelligence Oversight as the "fire alarm" model. If true, we will continue to witness an increase in oversight activity in this period after Snowden's disclosure and then an eventual decline. If the public demands more USIC oversight by its Congressional leaders, we will see an increased level of activity that will become the new normal.

Although the disclosures occurred almost two years ago, it is likely too soon to quantify the effect on lobbying, interest groups, or even on national elections. The defeat of Senator Mark Udall (D-Colorado) in the 2014 mid-term elections may signal it will be more of the same with intelligence matters and government oversight of the USIC not even entering into the voter's mind at the polls. Senator Udall, along with Senator Ron

Wyden (D-Oregon), has been too of the staunchest supports of NSA reforms and USIC transparency.

CHAPTER THREE: *The non-Deterrent Effect of Prosecuting Media Leaks*

> "I hate newspapermen. They come into camp and pick up their camp rumors and print them as facts. I regard them as spies, which, in truth, they are. If I killed them all there would be news from Hell before breakfast."
>
> –William Tecumseh Sherman

INTRODUCTION

Although today's security and counterintelligence officials may not make jokes about killing journalists as Sherman did, the publication of classified intelligence by media outlets have become a thorn in their side. With the introduction of the twenty-four hour news cycle, daily perusal of almost any media outlet's publication will encounter at least one article attributed to "unidentified government sources" or "unidentified intelligence officials" and purportedly containing classified intelligence. The unauthorized disclosure of classified information to a media outlet is referred to as a "media leak." The perceived increase in prosecutions of individuals allegedly responsible for media leaks by President Barack Obama's Administration generated a political firestorm with security and counterintelligence officials frantically investigating each leak and looking to ways to stop the unauthorized disclosures on one side and advocates of free speech and government transparency on the other.

Security and counterintelligence officials argue the alleged unauthorized

disclosure of classified information to the media (or anyone for that matter) causes grave harm to our national security. In a speech delivered to the Heritage Foundation, Chairman of the House Select Committee on Intelligence, Representative Pete Hoekstra, clearly stated that "some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information."[100] In response to the recent publication of thousands of classified documents on the WikiLeaks' website and other unauthorized disclosures, the Office of Management and Budget issued Memorandum M-11-06 directing "departments and agencies that handle classified national security information to establish assessment teams (consisting of counterintelligence, security, and information assurance experts) to review their implementation of safeguarding procedures."[101]

Individuals condemning the prosecution of individuals accused of providing classified information without authorization includes scholars, media representatives, lawyers and advocacy groups. Although each group or person has their own reason for condemning prosecution of media leak cases, former Assistant Attorney General Kenneth L. Wainstein alleges defense attorneys typically challenge the government's case by "invoking everything from first amendment principals to allegations of improper classification to arguments that their client's alleged leak was actually an authorized

[100]Pete Hoekstra, *Secrets and Leaks: The Costs and Consequences for National Security,* July 29, 2005, accessed August 8, 2011, http://www.heritage.org/research/reports/2005/07/secrets-and-leaks-the-costs-and-consequences-or-national-security.

[101] Jacob J. Lew, *Memorandum M-11-08*, January 3, 2011, accessed August 21, 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-08.pdf.

disclosure within the scope of his or her official duties."[102] There are also individuals who believe individuals who leak classified information should be sanctioned, but mitigate the crime by saying most "leakers" are well-intentioned government servants who did not intend to harm the national interests. This group proposes fines or administrative actions including the loss of security clearance as the suggested punishment. Although the leaking of information to the press is nothing new, the recent and frequent rise in the number of media leaks and subsequent increase in prosecutions is cause for alarm on both sides.

In this chapter, I attempt to sort out verify the claims of media and transparency advocates that prosecuting media leaks stifles freedom of speech and deters would be leakers and whistleblowers from coming forward. I initiated my research by investigating deterrence and theories of deterrence. In addition to defining deterrence and reviewing theory, I also researched the "anatomy" of a media leak investigation to understand the process by which they are referred, investigated, and potentially prosecuted. By understanding these topics, I hypothesized prosecuting media leaks would not have a deterrent effect.

Using publically available statistics illustrated in Table 7 and 8, I effectively proved the likelihood of being identified as a leaker was less than 8% and the likelihood of being prosecuted was even less. Moreover, I reviewed several of the recent publicized

[102]Kenneth L. Wainstein, *Federation of American Scientists,* May 12, 2010, accessed July 21, 2011, http://www.fas.org/irp/congress/2010_hr/051210wainstein.pdf.

to cases to understand to determine whether the cases matched the criteria for deterring would be leakers at least according to current deterrence theory. Application of deterrence theory to the case studies clearly indicate that prosecuting individuals accused of leaking classified information to the media does not meet the thresholds of having a deterrent effect on would be leakers. If anything, the prosecution of alleged leakers most likely provides a roadmap would would-be leakers to avoid getting caught.

DETERRENCE THEORY

With the media frenzy created by the perceived and recent increase in prosecutions of individuals accused of providing classified information to media representatives without authorization, one must ask himself/herself if prosecution of those accused of this crime sufficiently deters others from engaging in similar illegal behavior. Although the topic of media leaks presents multiple research opportunities, the focus of this analysis is the deterrent effect of recent media leak prosecutions. To conduct the described analysis, this chapter begins with a historical summary of law enforcement deterrence and subsequently reviews available scholarly literature on the topics of deterrence, effective prosecution, organizational bureaucracies, and procedures for protecting classified information at trial.

The earliest literature describing the subject of law enforcement in economic terms can be traced to the eighteenth century writings of Montesquieu (1748), Cesare Beccaria (1767), and Jeremy Bentham (1789). Without explanation, scholarship associating law enforcement and economics laid dormant until the publication of Gary S.

Becker's *Crime and Punishment: An Economic Approach*.[103] Although Becker's analysis of law enforcement in terms of economics formed the basis for scholarship from which most deterrence and optimal enforcement studies are derived, most criminologists accept Beccaria's assertion in *Of Crimes and Punishment* (1764) that potential criminals will be deterred only if punishment for commission of a crime is administered quickly, with certainty, proportionately and publicly.[104]

Recognizing Beccaria's "four pillars" represented an idealist view of criminal deterrence, Becker developed formulas using input data contained in crime rates, prison population, and the monetary costs associated with law enforcement and prosecution to identify the social cost of criminal behavior. Since its publication in 1968, Becker's representation of the economic costs associated with illegal behavior and law enforcement provided a framework for resource allocation and policy debate to combat criminal activity based on factors.[105] By representing law enforcement in economic terms, Becker put a price tag on Beccaria's "four pillars."

Becker's comprehensive study of law enforcement is the basis for studies in optimal law enforcement whereas researchers or politicians attempt to optimize resource

---

[103]A. Mithchell Polinsky and Steven Shavell, "The Economic Theory of Public Enforcement of Law," *Journal of Economic Literature* Vol. 38, No. 1 (Mar., 2000): 45, accessed July 5, 2011, http://www.econ.boun.edu.tr/zobuz/teaching/EC352/polinsky_shavell(1).pdf.

[104]Rudolph Gerber and John Johnson, *The Top Ten Death Penalty Myths: The Politics of Crime Control* (Westport: Prager Publishers, 2007), 68-69.

[105]Gary S. Becker, "Crime and Punishment: An Economic Approach," *Journal of Political Economy (*1968):170.

allocation based on net social cost identified by comparing the cost of enforcement with economic loss of particular crimes. Although worth mentioning, the subject of optimal enforcement is tangential to the research question of this paper. Disregarding the economics of optimal law enforcement, Becker's research verified Beccaria's assertion that by probability and severity of punishment deters potential criminals. Over the last four decades, scholars have debated Becker's the applicability of the data used in Becker's analysis and the conclusions reached. Becker's economic analysis has been criticized and supported through scholarly research in the fields of criminal deterrence and law enforcement.

Becker's analysis is limited by the used of incomparable crime figures. In Becker's essay, input figures include crime rates, economic costs and incarcerations rates for robbery, burglary and larceny. Becker correctly identifies robbery as crime against a person and burglary and larceny as property crimes without commenting on the possible effect of comparing dissimilar crimes. Although outside the purview of this review, one can reasonably assume the incarceration rate and length of prison sentence for a crime against a person is higher than a property crime based on the likelihood of the perpetrator can be identified by a victim witness. Therefore, subsequent research which re-analyzes the Beckerian model is limited by the same inputs.

Although outside the scope of this analysis, it is worth noting that Becker's inputs for cost of law enforcement are limited by the era of his study. Although costs associated with law enforcement have certainly inflated since 1968, the evolution of social media

and the founding of neighborhood watches and watchdog groups such as the Guardian Angels and Perverted-Justice allow law enforcement to more effectively prioritize resources.

Since Becker's application of economic theory to deterrence in 1968, scholars focused research on three of Beccaria's "four pillars" to determine which one most effectively deters would-be criminals: severity, certainty or celerity. To date, there has been limited, if any, research on the deterrent effect of publicity in deterring illegal behavior. In order to determine which, if any, of the pillars produces a significant deterrent effect, it is necessary to evaluate scholarly literature published since Becker's essay.

As part of their research into the deterrent effect of perceived severity, Grasmick and Bryjak identified twelve studies measuring the perceived certainty and perceived severity of legal sanctions (Anderson et al.: Bailey and Lott; L. Cohen; Jensen and Erickson; Kraut; Meier and Johnson; Minor; Silberman; Teevan, a,b,c; Waldo and Chiricos). Based on their evaluation of the data contained in these studies, Grasmick and Bryjak determined only Kraut's study identified any link between perceived severity and deterrence.[106] Grasmick and Bryjak noted that "although some effort has been devoted to refining the measurement of perceived certainty of punishment, no such attempt has been made to develop a theoretical and empirically sound measure of perceived

[106]George J. Bryjak and Harold J Grasmick, "The Deterrent Effect of Perceived Severity of Punishment," *Social Forces* (1980): 472, accessed July 14, 2011, http://www.jstor.org/stable/2578032.

severity.[107] Rather than using incarceration rates and crime statistics as Becker did in 1968, Grasmick and Bryak noted current deterrence scholarship utilized surveys (verbal and written) of would-be criminals to determine their knowledge of current legal sanctions and their perception of expected sanctions given a particular crime. In particular, Grasmick and Bryak noted the majority of the research regarding perceived severity produced inconsistent results based on the subjective nature of the questions

Based on the findings of their research, Grasmick and Bryak hypothesized "the severity of punishment (S) is inversely related to involvement in illegal behavior (l), but only among those people who perceived the certainty of arrest to be relatively high."[108] To test their hypothesis, the pair conducted interviews of four hundred randomly selected individuals and interviewed them regarding their perceptions of legal sanctions. Rather than asking respondents if arrest would result in a jail sentence, Grasmick and Bryak requested respondents to imagine the likely sentence for a crime (theft, illegal gambling, tax cheating, hurting someone, littering, illegal fireworks, and drunken driving) and then asked how much of an imposition the anticipated sentence would cause in their life. By personalizing the research question to the respondent's life, Grasmick and Bryak removed the subjectivity of a jail sentence. Ultimately, Grasmick and Bryak concluded

[107]George J. Bryjak and Harold J Grasmick, "The Deterrent Effect of Perceived Severity of Punishment," *Social Forces* (1980): 474, accessed July 14, 2011, http://www.jstor.org/stable/2578032.

[108]George J. Bryjak and Harold J Grasmick, "The Deterrent Effect of Perceived Severity of Punishment," *Social Forces* (1980): 477, accessed July 14, 2011, http://www.jstor.org/stable/2578032.

that perceived severity of punishment is high amongst those who believed the certainty of punishment is high.

Grasmick and Bryak's findings are based on analysis of responses to the perceived severity of sanction based on hypothetical arrest for a variety of property crimes. While the questions from the data section of their study were altered to avoid perceived flaws in previous studies, the phasing resulted in the dependence of the severity of punishment on the certainty of punishment. The described dependence limits the study's ability to ultimately determine if either certainty of punishment or severity of punishment is a more effective deterrent.

Based on their analysis of previous research, Maxwell and Gray determined significant research indicated criminals were first deterred by the perceived certainty of punishment and then by the perceived severity of punishment but only if the would-be offender perceived potential activity would result in certain punishment.[109] Maxwell and Gray determined studies examining the perceived certainty of sanctions are limited in "establishing the time-order between perceptions of the certainty of punishment and criminal behaviors" and "in using samples that were not generalizable to the offending population."[110]

---

[109]Sheila Royo Maxwell and M. Kevin Gray, "Deterrence: Testing the Effects of Perceived Sanction Certainty on Probation Violations," *Sociological Inquiry* Vol. 70, No. 2 (Spring, 2000): 120, accessed July 7, 2011, http://onlinelibrary.wiley.com.proxy1.library.jhu.edu/doi/10.1111/j.1475-682X.2000.tb00901.x/pdf.

[110]Ibid, 131.

In order to identify the deterrent effect of perceived certainty of punishment, Maxwell and Gray analyzed data from Intensive Supervision Probation program where inmates consisted of individuals who were previously convicted of either drug or property crimes. Maxwell and Gray queried respondents to determine the likelihood of failure enrolled in this program. To account for the time-order issue Maxwell and Gray perceived to limit previous studies, their study evaluated the respondents' perception as to how many failed drug tests would be allowed at the start of the program, possibility of a savvy person to pass the mandatory drug tests, and their attitude towards requirements of the program. Based on the respondent's enrollment in the legal system as a probationer, the threat of sanction was a reality as opposed to previous studies where the certainty of punishment was merely theoretical.[111]

The result of Maxwell and Gray's research was far from certain. Although the research indicated a deterrent effect of the perceived certainty of punishment, the actual effect was biased by the variables of race, ethnicity and age. Ultimately, Maxwell and Gray's research identified the need for further research on the topic accounts for the variant effects of demographics.

Maxwell and Gray eliminated the perceived theoretical limitation of previous studies by using a test group consisting of individuals in a program where failure results in guaranteed sanction absent increasing severity of punishment. While relevant to drug

[111]Ibid, 132.

treatment or other rehabilitation programs, the study is limited in its applicability to deterrence studies for involving individuals outside of the criminal process.

As a result of his research into the possible deterrent effects in death penalty cases, Bailey noted previous studies failed to include the deterrent effect of celerity or timeliness of administering sanctions. By ignoring the potential deterrent effect of celerity in death penalty cases, Bailey identified a possible bias in previous studies. In addition, Bailey determined the results of some studies were biased based on the inclusion of data from states where the death penalty is illegal.[112] Therefore, Bailey focused his research and analysis on the deterrent effect of celerity in death penalty cases in states where the sanction is legal.

Federal Bureau of Investigation statistics for murder and non-negligent manslaughter were used as indicators of capital homicide rates. Bailey identified the certainty of executions using averages from three compilations of execution rates and the celerity of executions using average median time between sentencing and execution. Six socio-demographic factors were used to control for possible ambiguity.

Analysis of data collected by Bailey revealed a negligible deterrent effect of severity and certainty of punishment and absolutely no deterrent effect of celerity of punishment in death penalty case. Bailey acknowledges the results of his work confirms the accuracy of earlier studies. In mitigation, Bailey identifies the infrequent use of the

[112]William C. Bailey, "Deterrence and the Celerity of the Death Penalty: A Neglected Question in Deterrence Research," *Social Forces* Vol. 58, No. 4 (June, 1980): 1311, accessed on July 1, 2011, http://www.jstor.org/stable/2577328.

death penalty and the length of time between sentencing and execution as the likely reason for negative deterrent effects.[113]

Unlike previous research, Bailey correctly limits his input data to statistics from states where the death penalty is legal. Although Bailey recognizes possibly limitations created through his input of data including the time between sentencing and execution, he does not propose another timeframe he considers useful in the study of celerity.

Although much of Bailey's research into law enforcement deterrence focuses on the deterrent effect of the death penalty, he wisely researches different possibilities for its deterrent effect. Unlike the review described above, Bailey alleges, "The deterrent effect of criminal law is dependent upon communication to the public of the threat and application of sanctions."[114] Bailey focused his research on the media attention given to executions and its perceived effect on homicide rates.

Bailey's analysis of previous research indicated homicide rates were previously compared to execution publicity in newspapers or print media. Statistics collected indicated individual most likely to commit capital offenses received news by watching television and not print media. Therefore, Bailey argued previous research was invalid. To make his research relevant to the times, Bailey's data included statistics on television

[113]William C. Bailey, "Deterrence and the Celerity of the Death Penalty: A Neglected Question in Deterrence Research," *Social Forces* Vol. 58, No. 4 (June, 1980): 1329-1330, accessed on July 1, 2011, http://www.jstor.org/stable/2577328.

[114]William C. Bailey, "Murder, Capital Punishment, and Television: Execution Publicity and Homicide," *American Sociological Review* Vol. 55 (Oct., 1990): 628, accessed July 1, 2011, http://www.jstor.org/stable/2095860.

coverage of executions versus homicide rates corresponding to the described coverage. Bailey concluded the publicity of executions did not have a deterrent effect on homicide rates. Regardless of the graphic nature of the coverage, Bailey determined the television coverage actually showed execution is neither certain or timely.[115]

While statistics indicating individuals most likely to commit a capital crime received news updates from television broadcast guided Bailey's research, Bailey did not account for the sub-set of this demographic that actually watches television news broadcast. While more relevant than previous research conducted using publication statistics for print media, Bailey's lack of accounting this sub-set of would-be criminals that actually watch television news broadcast. In addition, the internet has overtaken television as the most watched source of news coverage since the publication of Bailey's work.

Based on the lack of resources, effective prosecution of criminals allows law enforcement entities to allocate resources accordingly. While not every case investigated results in charges filed, the government's goal should be a one-hundred percent conviction rate for cases prosecuted. Regardless of whether a case deliberated by judge or jury, the verdict is based on an evaluation of evidence presented at trial.

In her article, Janet Barbeau argues physical evidence rather than witness testimony is the key to an effective prosecution. If collected properly and completely, physical evidence can form the basis for a jury's decision. Based on its importance,

[115]Ibid.

Barbeau notes the importance of locating and collecting evidence for a case. Barbeau alleges enforcement agencies must be familiar with entities and available resources within their domain. In addition, enforcement agencies must employee individuals capable of utilizing the most advanced and certified collection techniques that ultimately will present the most compelling evidence.[116] Recognizing the importance of physical evidence collection and presentation in effective prosecutions, Alabama Governor Bob Riley provided state attorneys with a $110,000 grant in 2006 to provide training involving the "effective questioning of experts, proper search and seizure, legal updates and methods in jury selection."[117]

Although prosecutions can fall apart for any number of reasons prior to trial, Barbeau rightfully alleges the most important element in an effective prosecution is evidence. Barbeau presents logical means by which enforcement agencies can identify, collect and present evidence prior to and during trial. However, without statistics or case studies to back her assertions, Barbeau's article is merely a guide to effectively prosecuting criminals.

Although the FBI is authorized to investigate media leaks under Executive Order 12333, media leak investigations are often limited by the evidence available to identify

[116] Janet Barbeau, "Evidence and Property Control," Law & Order, Vol. 51, No.8 (Aug 2003): 96-97, accessed August 21, 2011, http://search.proquest.com/docview/197229977/fulltextPDF?accountid=11752.

[117] "Gov. Riley Awards Grant for More Effective Dui Prosecution," *US Fed News Service, Including US State News,* Nov 03, 2006, accessed August 21, 2011, http://search.proquest.com/docview/469786314?accountid=11752.

the perpetrator.[118] The reactive nature of media leak investigations forces investigators to rely heavily on electronic audit records. Typically, the evidence of the crime can be found in building access records, building surveillance video, telephone records, official e-mail header information and content, and document access records. In most cases where the FBI is able to identify a subject, the alleged suspect utilized an official telephone or e-mail account to contact the journalist who published the information. Although the FBI can seek the issuance of Grand Jury subpoena to obtain a reporter's telephone or e-mail records, the use of this technique requires authorization by the Attorney General and is not approved in every case.[119]

Although suspects of criminal activity are not always affiliated with an organization or entity, investigative agencies often have to coordinate with multiple entities to collect evidence in support of criminal cases. In the case of a homicide, the police department must coordinate evidence collection with the County (or other) Medical Examiner (ME). In the case of a moving violation (traffic ticket), the police must coordinate with the court and the prosecution. Based on the coordination amongst various entities that do not necessarily fall under the same chain of command or share the same mission, it is important to understand the conflicts of bureaucratic politics.

[118]Lisa O. Monaco, "Unauthorized Disclosure of Classified Information," Federation of American Scientists Web site, February 9, 2012, 3, accessed March 15, 2015, http://fas.org/irp/congress/2012_hr/020912monaco.pdf .
[119]Lisa O. Monaco, "Unauthorized Disclosure of Classified Information," Federation of American Scientists Web site, February 9, 2012, 6, accessed March 15, 2015, http://fas.org/irp/congress/2012_hr/020912monaco.pdf .

Although countries like the United States have a common foreign policy, the organizations comprising the federal government have differing and often competing missions. In J. Garry Clifford's aptly titled essay, *Bureacratic Politics*, Clifford reviews Graham T. Allison's *Essence of Decisions* and attempts to explain the realities and complexities unique to the bureaucracy associated with the United States. Rather than evaluating historical events as a part of a common foreign policy, both Allison and Clifford suggest each event be analyzed through the eyes of the entities involved in supporting or responsible for the actions taken by the United States. Ultimately, "policy flows instead from an amalgam of large organizations and political actors who differ substantially on any particular issue and who compete to advance their own personal and organizational interests as they try to influence decisions."[120]

Without getting lost in the minutiae of historical foreign policy decisions, Clifford's essay eloquently identifies what some would described as a flaw in the bureaucracy of the United States government. Clifford acknowledges the United States government consists of various entities designed to support and execute various functions of United States foreign policy. Although the goal of the United States foreign policy is to promote its interest abroad, the various and sometimes competing missions of the entities of the government creates gridlock and internal conflict sometimes resulting in unnecessary delays in action or inaction.

[120] J. Garry Clifford, "Bureaucratic Politics," *The Journal of American History* Vol. 77, No. 1 (Jun., 1990):162, accessed August 21, 2011, http://www.jstor.org/stable/2078648.

"On those rare occasions when there is an identifiable leaker, the government must still decide whether prosecuting would mean divulging too many secrets to be worth it — starting, usually, with having to confirm in public that a particular leak was accurate."[121] Competing interests amongst the victim agencies in leak cases is one the reasons leak investigations rarely move forward, and precisely the reason prosecutions drag on for years. The evolution of a leak case is important to understanding how competing organizational interests could affect the advancement of a case.

According to the testimony of Robert S. Mueller III, the Director of the FBI, before the United States Senate Judiciary Committee on September 16, 2009, Executive order 12333 (as amended) mandates members of the United States Intelligence Community (USIC) report violations of law regarding the unauthorized disclosure of classified information to DOJ. The agreed mechanism for notifying DOJ of an unauthorized disclosure is memorandum (referred to as a crimes report) that includes the reporting agency's answer to the following eleven questions focusing on facts surrounding the disclosure:

1) Give the date and identity of the article disclosing the classified information?
2) Give specific statements in the article which are considered classified and whether the data was properly classified?
3) State whether the classified date is disclosed accurately?
4) State whether the data came from a specific document and, if so, the origin of the document and the name of the individual responsible for the security for the security [sic] of the classified data?

[121]Charlie Savage, "For U.S. Inquiries on Leaks, a Difficult Road to Prosecution," New York Times, June 9, 2012, accessed March 28, 2015, http://www.nytimes.com/2012/06/10/us/for-us-inquiries-on-leaks-a-difficult-road-to-prosecution.html?_r=0.

5) Give the extent of official dissemination of the data?
6) State whether the data has been subject of prior official release?
7) State whether prior clearances for publication or release of the information were sought from the proper authorities?
8) State whether the material, or portions thereof, or enough background data has been published officially or in the press to make an educated speculation on the matter possible?
9) State whether the data can be declassified for the purpose of prosecution, and, if so, the names of the person competent to testify concerning the classification.
10) State whether declassification has been decided upon prior to the publication of the release of the data?
11) What effect does the disclosure of classified material have on the national defense?[122]

Although most of these questions are germane to classification of the information, questions regarding the declassification of the information for prosecution and the effect of the disclosure on national defense are central to the progress of any leak investigation and prosecution. The answers to these questions are not simple and require careful evaluation of potential source compromise, and considerations of other potentially related ongoing operations, and potential damage to foreign relations, etc. Victim agencies can answer the information can be declassified, the information cannot be declassified for prosecution, or even they will consider declassifying the information. DOJ and FBI can decline referrals for any number of justified reasons, but the likely reasons cases referrals are declined based on issues which would make prosecution difficult. These include the information disclosed was too widely disseminated, incomplete or unavailable audit

[122]PBS, "Unauthorized Disclosure of Classified Information '11 Questions'," accessed June 17, 2011, http://www.pbs.org/wgbh/pages/frontline/newswar/art/leakp_large.jpg.

records for individuals accessing intelligence, and the victim agency's unwillingness to declassify the intelligence for use at trial.[123]

Depending on their evaluation of the responses to the 11 questions, DOJ may or may not refer the case to the FBI which possesses its own discretion to initiate an investigation. The predication for the investigation is based on the legal interpretation that the unauthorized disclosure of classified information to the media (an unauthorized recipient) is a violation of 18 U.S. Code § 793 - Gathering, transmitting or losing defense information. Upon initiating an investigation, the FBI must collect opens an umbrella investigation focused on the unknown subject alleged to have leaked the relevant information to a journalist of some sort. Media leak cases are similar to traditional espionage case in that the FBI knows certain information was compromised to someone not authorized to receive it. Unlike a traditional espionage case where the USIC might obtain SIGINT or HUMINT identifying the responsible party from intelligence collection efforts targeting adversaries of the United States, current law (freedom of the press, etc.) prevents the USIC from proactively collecting intelligence from journalists.

When the FBI is able to identify the individual(s) responsible for the unauthorized disclosure, the decision to prosecute is made through conference between the FBI, DOJ and the Assistant United States Attorney (AUSA) assigned to the case. Although the FBI can be certain the identified individual is responsible for the leak, the legal standard of preponderance of evidence is not always easy to attain in these types of case. Ultimately,

[123]Lisa O. Monaco, "Unauthorized Disclosure of Classified Information," Federation of American Scientists Web site, February 9, 2012, 4, accessed March 15, 2015, http://fas.org/irp/congress/2012_hr/020912monaco.pdf .

DOJ decides whether evidence supports prosecution. If DOJ supports the prosecution, the case moves forward. If not, the FBI provides the evidence to the subject's employer to support the appropriate administrative sanctions.

Although identifying the subject of a media leak investigation seems like the biggest hurdle, these efforts pale in comparison to the efforts required to prosecute the case. According to Wainstein, prosecuting leak cases face a myriad of obstacles including declassification of the compromised information or other discoverable materials and legal challenges filed by the defense.[124] Probably the most contentious obstacle to overcome is a defendant's right to a fair trial versus the need to protect classified information from disclosure during a public trial. Historically, the government has requested the substitution of redacted documents for original ones, substitutions of pseudonyms on documents and even shielding the identity of witnesses during trial in the case of individuals who are undercover.

The United States Congress enacted the Classified Information Procedures Act (CIPA) of 1980 to ensure the protection of classified subsequent to the publication of a criminal indictment. At the outset of the CIPA process (CIPA Section 3), the government files a motion requesting the district court issue a protective order limiting access to the court's proceedings and access to the classified information to only those with the proper

[124]Kenneth L. Wainstein, *Federation of American Scientists,* May 12, 2010, accessed July 21, 2011, http://www.fas.org/irp/congress/2010_hr/051210wainstein.pdf.

security clearances.[125] As defense counsel does not typically already possess a security clearance, the entire defense team must begin the process of obtaining a clearance before receiving any classified discovery from the government. According to the Office of the Director of National Intelligence, the longest processing time for the fastest 90% of Top Secret security clearance cases ranged from 73 days for the Department of State to 454 days for the Central Intelligence Agency.[126] Although this process could be expedited if under court's order to do so, the court often allows the process proceed naturally. Therefore, defense counsel could be precluded from receiving vital discovery for anywhere from 2 months to over a year.

After the designated defense counsel obtains the necessary security clearances, the CIPA process progresses to CIPA Section 4. This section revolves around the defendant's discovery rights and the prosecution's discovery obligations.[127] Under this section, the prosecution may file sealed motions requesting the judge's approval to withhold information collected during the course of the government's investigation. If the judge concurs with the government's motion(s), the prosecution can withhold the information. If the judge disagrees, a ruling ordering the production the material can be issued. In response to defense motions during CIPA Section 4, the prosecution evaluates the defense's request and then either turns over the requested items files a sealed reply

[125]U.S. Department of Justice, "Criminal Resource Manual 2054 Synopsis of Classified Information Procedures Act (CIPA)," U.S. Department of Justice Web site, 2, accessed March 1, 2015, http://www.justice.gove/usao/eousa/foia_reading_room/usam/title9/crm02054.htm.
[126] (Intelligence 2013)6.
[127] U.S. Department of Justice, "Criminal Resource Manual 2054 Synopsis of Classified Information Procedures Act (CIPA)," U.S. Department of Justice Web site, 3, accessed March 1, 2015, http://www.justice.gove/usao/eousa/foia_reading_room/usam/title9/crm02054.htm.

that includes reasons for not do so. The judge can either issue a ruling that confirms the prosecution's right to withhold that information or a ruling denying the prosecution's request. This process is ongoing and dependent on motions filed by the defense. With that said, every motion requires the judge to set a date for government reply and time for the judge to rule.

During CIPA Section 5 and Section 6, defense counsel typically files notice of intent to use certain classified information as part of the defense, as well as motions to suppress evidence. CIPA includes a series of motions and suppression hearing where the defense demands the government turn over certain information which CIPA created a process in which the prosecution and defense could present evidence to either be turned over in discovery or used in trial to present evidence and other discovery to review, evaluate which implemented closed court proceedings whereas the prosecution and defense teams introduce classified information each side expects to introduce at trial. Ultimately, the presiding judge weighs the evidence presented by both sides and rules on the manner in which the classified information will be introduced at trial. If the judge rules the defendant right to a fair trial is denied by redacting or substituting documents for the original classified documents, the prosecution must evaluate the damage to national security posed by public disclosure of the classified information by proceeding as mandated against dropping the charges or working out a plea bargain.[128]

[128]Charlie Savage, "For U.S. Inquiries on Leaks, a Difficult Road to Prosecution," New York Times, June 9, 2012, accessed March 28, 2015, http://www.nytimes.com/2012/06/10/us/for-us-inquiries-on-leaks-a-difficult-road-to-prosecution.html?_r=0.

Regardless of the strength of the government's case and barring a plea deal with the subject, one can expect the prosecution of a media leak case to take years.

THEORY AND HYPOTHESIS

Scholarly literature on the topic of law enforcement deterrence indicates theories first proposed by Beccaria in 1768 are relevant today. Beccaria proposed that potential criminals will be deterred only if punishment for commission of a crime is administered quickly, with certainty, proportionately and publicly. Deterrence studies have often focused on the effect of one or two of these pillars rather than testing all "four pillars."[129] Legal rights of the accused, legal maneuvering, and judicial scheduling would likely hinder any efforts to test all of the "four pillars" in a meaningful way and may indicate Beccaria's idea is applicable in theory as opposed to practically.

Applying the results of research described above to the deterrent effect of prosecuting media leak cases identifies a significant flaw in the research question initially proposed. The prosecution of a suspect is merely the legal process used to determine an individual's innocence or guilt. Ultimately, a suspect can be found innocent or guilty, can accept a plea bargain and in some cases the government can drop the charges.

Significant media attention has centered on the perception that the Obama administration increased prosecutions of individuals suspected of leaking classified information as part of a veiled some sort of government secrecy. Although the media

[129]Rudolph Gerber and John Johnson, *The Top Ten Death Penalty Myths: The Politics of Crime Control* (Westport: Prager Publishers, 2007): 68-69.

continues to push the message that prosecutions are politically motivated, Wainstein offers an alternative theory that the increased prosecutions can be attributed to better audit capabilities in the USIC.

Further, the review of literature regarding effective prosecution reveals that evidence collection and presentation is the key to conviction. However, recent cases such as WikiLeaks, clearly illustrate shortcomings in the government's ability to audit computer activity and collect evidence in support of prosecution(s) for unauthorized disclosures. Moreover, the bureaucratic infighting created by competing missions can be expected from agencies the FBI must work with to investigate these crimes.

The wisdom gained from review of available deterrence literature clearly indicates the deterrent effect associated with the perceived severity of prosecuting the unauthorized disclosure of classified information to representatives of the media (media leaks) is likely negated by the lack of certainty and celerity of administering sanctions. More explicitly and based on the wisdom gained from the review of topical literature, the perceived increase in prosecuting individuals suspected of leaking classified information will not have any measurable deterrent effect on potential leakers.

METHODOLOGY

As previously indicated, the purpose of this chapter is to determine if the perceived increase in prosecution of individuals accused of leaking classified information to the media acts as a deterrent to potential "leakers." To formulate the hypothesis for this research, scholarly literature on the deterrent effect of law enforcement, effective

prosecution, and "the anatomy" of a media leak investigation was reviewed and analyzed. With a better understanding of these cases and the issues involved, this chapter provide a summary review of the following media leak investigations that have been prosecuted or are currently being prosecuted: United States v. Jeffrey Alexander Sterling, United States v. Stephen J. Kim, United States v. Thomas Drake, United States v. Shemai Leibowitz, and United States v. John C. Kirakou. Of note, all five defendants in the captioned cases waived their right to a speedy trial.

It is worth noting that Samuel Morison was the first individual charged and ultimately convicted of disclosing classified information to *Jane's Defense Weekly* in 1985. Although worth noting, this chapter will not review the United States of America v. Samuel Morison case based on its historical nature, United States of America v. Bradley Manning because he was already incarcerated by the time the case was referred to the FBI and he was prosecuted under, the investigations of General Petraeus or Donald Sachtelben because they both pled guilty prior to being indicted, or the case of Edward Snowden because of his unlawful flight to avoid prosecution.

To put the perception the Obama Administration implemented a crackdown on media leaks in perspective, this chapter included the most recent and available media leak statistics (2005-2009) as reported by the Federal Bureau of Investigation (FBI) to the United States Congress as illustrated in Exhibit 1. Due to the classification of media leak statistics annually reported to the United States Congress by DOJ, this chapter uses the most recent and unclassified statistics as reported by the FBI.

The variables contained in the data will be the number of prosecutions and the number of unauthorized disclosures. If prosecuting media leak cases has a deterrent effect on potential "leakers," the data will indicate the number of leaks decreases as the number of prosecutions increase. If prosecution does not have a deterrent effect, the opposite will occur. The perceived increase in prosecution of media leaks occurs subsequent to the latest data contained in Table 1. Therefore, the statistics illustrated in Table 1 can support future studies involving the measurable deterrent effect of prosecution in the reviewed cases. Although studies of the deterrent effect of the described prosecutions are relevant and necessary, the results of any future endeavor should account for the prevention and deterrent effect associated with the issuance of Office of Management and Budget Memorandum M-11-06 in 2010.

MAIN DISCUSSION

As established in the deterrence literature, effective deterrence requires the punishment to be quick, certain, public and severe. To determine if prosecuting leakers has a deterrent effect, Table 7 illustrates the statistics involving the prosecution of media leaks over a five-year period (2005-2009)

YEAR	REFERRALS	LEAK INVESTIGATIONS	# OF SUSPECTS IDENTIFIED	SUSPECTS PROSECUTED DURING THIS TIME PERIOD
2005	**46**	**7**	**1**	**0**
2006	**29**	**9**	**5**	**0**

2007	**55**	**5**	**5**	**0**
2008	**23**	**3**	**1**	**0**
2009	**30**	**2**	**2**	**0**

Table 7: FBI Statistical Data on Leaks of Classified Intelligence Information[130]

Although the statistics illustrated are limited to a five-year period, they clearly illustrate the difficulties in investigating media leak cases. Of the 183 referrals between 2005 and 2009, the FBI only opened 26 cases or roughly 7 % of the time. Of the 26 cases opened, the FBI identified 14 subjects or approximately 54%. Although the FBI tends to do well identifying a subject if a case is initiated, the identification of only 14 subjects out of 183 referrals equates to identifying only 8% of the individuals responsible for unlawfully disclosing classified information. More astonishing is the fact that none of the subjects identified were indicted or otherwise charged in connected with the unauthorized disclosure during the time period represented in the table.

The table above clearly establishes the lack of certainty with regards to being criminally prosecuted for leaking classified to the media. However, the eleven individuals criminally prosecuted for disclosing classified information to the media might suggest the statistics are not in favor of the leakers. A closer look at the cases associated with individuals actually prosecuted for this crime is required to identify the celerity, severity, and publicity of their potential punishment.

ALLEGED LEAKER	DATE(S) OF LEAK	DATE CHARGED	STATUS	SENTENCE

[130] Robert S. Mueller III, *United States Government Printing Office,* June 4, 2010, accessed July 21, 2011, https:\GPO\HEARINGS\56529.TXT.

Daniel Ellsberg	June 13, 1971	June 28, 1971	Case Dismissed on May 11, 1973	Not Applicable
Samuel Morison	July-August 1984	Arrested October 4, 1984	On October 17, 1985, Morison was convicted of violating 18 USC § 793(d) and 18 USC § 793(e).	On December 4, 1985, Morison was sentenced to two year's incarceration. On January 20, 2001, President Bill Clinto pardoned Morison.
Thomas Drake		Indicted on April 15, 2010	On June 10, 2011, Drake pled guilty to Exceeding Authorized Use of a Computer, in violation of 18 U.S.C. § 1030.	On July 15, 2011, Drake was sentenced to one year of probation and 240 hours of community service.
Shamai Leibowitz	April 2009	Information filed on December 4, 2009	On December 17, 2009, Leibowitz pled guilty to violating 18 USC § 798(a).	On May 24, 2010, Leibowitz was sentenced to 20 months in prison followed by three years of supervised probation
Bradley Manning	2009-2010	Charged under UCMJ on May 29, 2010	On February 28, 2013, Manning pled guilty to ten counts related to his unlawful removal, retention and publication of classified information. On July 30, 2013, Manning	On August 21, 2013, Manning was sentenced to 35 years' imprisonment, reduction in pay grade, forfeiture of all pay and allowances, and a dishonorable

			was convicted of an additional twelve charges.	discharge from the US Army.
Stephen Jin-Woo Kim	June 11, 2009	Indicted on August 27, 2010	On February 7, 2014, Kim pled guilty to violating 18 USC §793(d).	On April 2, 2014, Kim was sentenced to 13 months of incarceration followed by 12 months of supervised released.
Jeffrey Sterling	January 2006	Indicted on December 22, 2010	On January 26, 2015, Sterling was convicted of nine counts of unauthorized disclosure of national defense information and other related charges.	On May , 2015, Sterling was sentenced to 42 months of incarceration.
John Kirakou	2008 to 2009	Criminal Information filed on January 19, 2012	On October 23, 2012, Kiriakou pled guilty to violating Title 50 USC § 421(b)	On January 25, 2013, Kiriakou was sentenced to 30 months of incarceration.
Donald Sachtleben	May 2012	Child Pornography complaint filed May 15, 2012.	On September 23, 2013, Sachtleben pled guilty to violating 18 USC § 793(d)	On November 14, 2013, Sachtleben was sentenced to 43 months of incarceration.
Edward Snowden	May 20, 2013	Criminal Complaint filed on June 14, 2013	Not Applicable	Not Applicable
David Petraeus	August 2011	Not Applicable	On March 3, 2015, Petraeus pled guilty	On April 23, 2015, Petraeus

			to violating 18 USC § 1924	was sentenced to two years of probation and ordered to pay $100,000. Fine.

Table 8: Eleven known prosecutions involving the Unauthorized Disclosure of Classified Information to the Media[131]

Of the eleven cases illustrated in Table 8, six resulted in guilty pleas, three resulted in conviction, one case was dismissed, and one alleged leaker (Snowden) has avoided prosecution through flight. Four of the six guilty pleas involved admission and sentencing for committing felonies with an average incarceration of approximately twenty-six months. The leakers pleading guilty to misdemeanors have been sentenced to terms of probation and thus avoided jail time. Of the three defendants who have been convicted, Manning was sentenced to thirty-five years of incarceration (10 counts from guilty plea and 12 counts from guilty verdict), Morison was sentenced to two years of incarceration, and Sterling was sentenced to 42 months of incarceration.

These statistics clearly illustrate the likelihood of criminal sanctions is fairly high for individuals charged with criminal violations associated with their unauthorized disclosure. In fact, nine of the eleven individuals or 81.8% were criminally sanctioned for their actions. The potential resolution of the case against Snowden can only increase the likelihood of criminal sanctions for individuals charged.

[131]Steven Aftergood, "Selected Judicial Branch Documents on Secrecy, Leaks, Intelligence and Freedom of Information," Federation of American Scientist Web site," June 5, 2014, accessed May 1, 2015, http://fas.org/sgp/jud/.

The statistics from Table 7 clearly illustrate the unlikelihood of prosecution, as well as the potential for prolonged legal process in the cases that are prosecuted. However, it is important to analyze a few of those cases to identify reasons for the delays and potential remedies. For this reasons, this chapter will review the following cases: United States of America v. Jeffrey Alexander Sterling, United States of America v. Stephen Kim, United States of America v. Thomas Drake, United States of America v. Shemai Leibowitz, and United States of America v. John Kiriakou.

In case United States of America v. Jeffrey Alexander Sterling, the United States government indicted Sterling on December 22, 2010, on ten counts associated with the unauthorized disclosure of classified information to an identified reporter. The indictment alleges Sterling provided classified information including details of a CIA-sponsored covert program targeting the weapons capabilities of an identified country without authorization to an identified reporter in early 2003 and again circa 2005 or 2006. Careful review of the charging document reveals Sterling likely disclosed the classified information in retaliation for the dismissal of Sterling's racial discrimination lawsuit against the CIA and due to the CIA's refusal to allow Sterling to publish his memoirs.[132]

The five to seven year laps between the date(s) of Sterling's disclosures and the date of his indictment is of particular note. This time lapse can likely be tied to internal debates within the USIC about the ramifications of prosecuting Sterling including the likelihood of disclosing additional classified information at trial and the issues

[132] "*United States of America v. Jeffrey Alexander Sterling.* 1:10-cr-00485-LMB," Federation of American Scientist Web site, December 22, 2010, accessed May 1, 2015, http://fas.org/sgp/jud/sterling/.

surrounding the issuance of a subpoena to the article and book's author. Risen was initially served with a grand jury subpoena in 2008; however, he fought the subpoena and the government was able to secure an indictment two years later without his testimony.[133]

Issues involving Risen's potential appearance as a trial witness delayed the case for over four years after Sterling's indictment. In January 2015, the US Court of Appeals for the Fourth Circuit ruled a journalist's privilege did not trump subpoena compliance; thus paving the way for Risen's use as government witness. In a remarkable turn of events, the prosecution decided Risen would not be called to testify.[134] The four-year trial delay involving the Risen's potential testimony masked the effect of the CIPA process on the trial. Defense motions, government filings, and Court opinions issued through the CIPA process span approximately two and one half years from the date of Sterling's indictment.[135]

On August 27, 2010, the United States government charged Kim with two criminal counts relating to the unauthorized disclosure of national defense information to a media representative (United States of America v. Stephen Kim). As a result of Kim's alleged disclosure, the government alleged an identified journalist authored an article containing SIGINT and HUMINT circa June 2009. Based on a review of a website

[133]Matt Apuzzo, "Times Reporter Will Not Be Called to Testify in Leak Case," New York Times, January 12, 2015, accessed March 1, 2015, http://www.nytimes.com/2015/01/13/us/times-reporter-james-risen-will-not-be-called-to-testify-in-leak-case-lawyers-say.html?_r=0.
[134]Matt Apuzzo, "Times Reporter Will Not Be Called to Testify in Leak Case," New York Times, January 12, 2015, accessed March 1, 2015, http://www.nytimes.com/2015/01/13/us/times-reporter-james-risen-will-not-be-called-to-testify-in-leak-case-lawyers-say.html?_r=0.
[135]Steven Aftergood, "Selected Judicial Branch Documents on Secrecy, Leaks, Intelligence and Freedom of Information," Federation of American Scientist Web site," June 5, 2014, accessed May 1, 2015, http://fas.org/sgp/jud/.

dedicated to promoting Kim's legal defense, www.stephenkim.org, it becomes apparent Kim's defense team intends to challenge the government's case on the grounds of Kim's first amendment rights to speak with the press and questioning whether the information allegedly revealed was properly classified. [136] As discussed above, Wainstein alleges both potential challenges by the defense team are two of them most commonly used in media leak case and the two that present the biggest hurdles for the government to overcome.[137]

Although not as lengthy as the time frame between Sterling's disclosure and indictment, Kim's indictment lagged his alleged disclosure by approximately 14 months. The CIPA and discovery process played out for Kim from the time he was indicted until the time he pled guilty and later sentenced in April 2014, which was a time lapse of over four years from the date of his unauthorized disclosure. Kim was sentenced to 13 months of incarceration followed by 12 months of supervised released for violating 18 USC SS 793(d).[138]

On April 15, 2010, a grand jury indicted former National Security Agency (NSA) official, Thomas Drake, on ten charges related to his alleged disclosure of classified information to a journalist in 2006 and 2007. In court proceedings, Drake's defense team

[136]Abbe D. Lowell, *StephenKim.org,* accessed July 20, 2011, http://www.stephenkim.org/case.html.

[137]Kenneth L. Wainstein, *Federation of American Scientists,* May 12, 2010, accessed July 21, 2011, http://www.fas.org/irp/congress/2010_hr/051210wainstein.pdf.

[138]Ann E. Marimow, "Ex-State Department adviser Stephen J. Kim sentenced to 13 months in leak case," Washington Post, April 2, 2014, accessed March 1, 2015, http://www.washingtonpost.com/world/national-security/ex-state-dept-adviser-stephen-j-kim-sentenced-to-13-months-in-leak-case/2014/04/02/f877be54-b9dd-11e3-96ae-f2c36d2b1245_story.html.

refuted the government's allegations that Drake disclosed classified information. Although Drake's attorneys conceded Drake corresponded with the identified reporter, the defense described Drake as a whistleblower whose disclosures related to fraud and abuse at NSA rather than the disclosure of classified information.[139]

During the Classified Information Protection Act (CIPA) proceedings for the case, the presiding judge ruled the government needed to use more descriptive substitutions in its exhibits. After evaluating the available options, the government determined the parameters set forth would result in the additional release of classified information. After the government withdrew the original indictment against him, Drake plead guilty to one charge of intentionally exceeding the authorized access of a computer on June 10, 2011. Drake was later sentenced to one year of probation and community service.[140] Although Drake did not receive a jail sentence for the crime he admitted, Drake previously had his security clearance revoked, was terminated from his employment at NSA and lost his government pension as a result of the government's investigation.

Based on the time lapse between the disclosure date and date of indictment, the Drake case illustrates the investigative difficulties of identifying a subject and the potential bureaucratic infighting as it relate to using classified information in furtherance of prosecution. The 14th month time lapse between Drake's indictment and guilty plea

[139]Scott Shane, "Former N.S.A. official is charged in leaks case," *New York Times*, April 15, 2010.

[140] Federation of American Scientists, "Project on Secrecy," accessed July 21, 2011, http://www.fas.org/sgp/jud/drake/061011-dismiss.pdf.

illustrates both the delays of the CIPA process and potential obstacles to prosecution. Although appropriate for the crime in which Drake pled guilty, the sentence which included no jail time fails to meet the severity pillar of deterrence.

Although Shemai Leibowitz was employed by the FBI as a contract linguist for only eight months during 2009, the FBI alleged Leibowitz provided classified information to a person not authorized to receive the information. Based in part on the strength of the government's case, Leibowitz pled guilty to providing classified to an internet blogger during April 2009.[141] Although Leibowitz accepted responsibility for his actions at the time of sentencing, Leibowitz claimed he was a whistleblower and mitigated his actions by saying he disclosed the information based on his belief that he uncovered violations of law. Ultimately, Leibowitz was sentenced to 20 months in prison followed by three years of supervised probation.

On January 19, 2012, the United States government filed a criminal complaint and arrest warrant alleging John Kiriakou violated of Title 18, United States' Code, Sections 793(d) and 1001(a)(1), and Title 50, United States Code, Section 421(b). Specifically, the government alleged Kiriakou disclosed the identities of covert US government

[141]Federal Bureau of Investigation: Baltimore Division, "Former FBI Contract Linguist Sentenced for Leaking Classified Information to Blogger," accessed July 21, 2011, http://www.fbi.gov/baltimore/press-releases/2010/ba052410.htm.

employees involved a classified program to a news reporter without authorization between 2008 and 2009.[142]

Mr. Kiriakou had vowed to fight. But his chances were weakened after Judge Brinkema ruled on Oct. 16 that prosecutors needed only to prove that Mr. Kiriakou had "reason to believe" that the information he disclosed could be used to harm the country, not that he had intended to damage national security.

RESULTS AND CONCLUSION

As illustrated by the statistics in Exhibit 1, a significant number of media leak investigations are referred to the FBI by DOJ every year. Absent from these statistics due to the classification of the information is the number of cases that are referred to DOJ. As described above, cases are first referred to DOJ for evaluation by the victim agency or the Director of National Intelligence (DNI). Based on the merits of each crime's report, DOJ then forwards the referrals meeting the minimum standards for initiating an investigation. Although the referred crime's reports meet DOJ minimum standard for case initiation, the FBI evaluates each case prior to opening.

As the statistics illustrate, the FBI initiated cases on only 26 out of 183 cases referred. During the reporting period, the FBI identified suspects in 14 of the 26 cases. However, none of the identified 14 suspects were prosecuted during the reporting period. Although some may question the relevance of using statistics that don't include

[142]Joseph Capitano, "John Kiriakou Complaint - US Department of Justice," U.S. Department of Justice Web site, January 19, 2012, accessed March 1, 2015. http://www.justice.gov/sites/default/files/opa/legacy/2012/01/23/kiriakou-complaint.pdf. (Capitano 2012)

prosecutions, the lack of statistics is relevant to the research question as it relate to Beccaria's initial assertion that criminal sanction act as a deterrent only if and when the "four pillars" are applied.

Superficially, the statistics seem to support the mantra of the Obama administration war on journalists and free speech. Upon careful review of the case studies and cases mentioned but not reviewed, the fact is that most of those cases involve disclosures occurring outside of the date(s) covered by the statistics or the length of investigation prevented indictments or other legal process from occurring during the time. Although the statistics provide a basis for the extrapolation indicating an increase in media leak prosecutions, the statistics fail to indicate the reason for the lack of prosecution. Most likely, the DOJ and FBI agreed the evidence in the ongoing investigations was not strong enough to indict a perpetrator or the collection of evidence is ongoing.

Review of recent media leak cases revealed a lengthy process complete with obstacles including defense challenges and classification issues. Of the four cases reviewed, three cases resulted in the indictment of a suspect 14 months or longer after the alleged disclosure occurred. Unlike the other 3 cases, Leibowitz was sentenced within 13 months of his disclosure based on his acceptance of a plea bargain. The statistics illustrated in Exhibit 1 and the six case studies clearly indicate a lack of certainty in criminal punishment. The case studies from this chapter clearly indicate sentencing for individuals convicted (or pleading guilty) of crimes associated with unauthorized

disclosures vary from probation with community service to prison terms of approximately three years or less, which is far less than the allowable 10 year sentence.

As evident above, guilty pleas and/or convictions in cases involving unauthorized disclosure of classified information to the media are typically a fraction of the sentences given to convicted spies. The prosecution of leakers under the same laws as the government prosecutes spies is of great debate. On one side, free speech advocates and the media attempt to paint all leakers as whistleblowers on condemn their prosecution as draconian. On the other, there are those like Representative Hoekstra who realize leakers have done more damage to the USIC than those spying for a foreign government.[143] Spies typically disclose their secrets to a single service, which may or may not share that information with other liaison services. By releasing their information to the media, the classified information is released to the world's intelligence agencies as well as the world's population. Although important to mention for this chapter, the debate about the appropriate censure for leakers is a topic for future research and debate.

A review of the media coverage for each of the identified cases and leaks in general finds media coverage tends to criticize the government's prosecution of those accused or convicted of crimes associated with leaking providing classified information rather than the individual who allegedly leaked the information or admonishing the action

[143] Pete Hoekstra, *Secrets and Leaks: The Costs and Consequences for National Security,* July 29, 2005, accessed August 8, 2011, http://www.heritage.org/research/reports/2005/07/secrets-and-leaks-the-costs-and-consequences-or-national-security

of leaking information that could be detrimental to our national security.[144] Based on the perceived bias of media coverage, it appears the public (including potential leakers) are not educated of the potential repercussions of potential disclosures. Adequate media coverage would inform the public of the potential and likely sanctions imposed for the unauthorized disclosures, as well as educating the public as to the potential monetary and national security losses incurred as a result of SIGINT compromise or the loss of life resulting from compromise of HUMINT.

Evaluating the data indicates the original hypothesis for this chapter was accurate. Based on statistics, punishment resulting from media leak investigations cannot be described by any of Beccaria's "four pillars." In these cases, punishment is not applied with certainty, severity, celerity or publically. Without possessing any of these qualities consistently, prosecuting media leak cases does not meet the threshold for deterring would-be leakers.

Although the data presented clearly illustrates the characteristics of leak prosecutions do not meet the threshold for Beccaria's deterrence theory, it is important to acknowledge the subjective deterrent effect of the 8% chance of being identified as a leaker of classified information. Although the chances of being prosecuted for the unauthorized disclosure is even more remote than simply being identified as the leaker, would-be leakers could also be deterred by potential job loss, the loss of professional reputation, security clearance, and in some cases reduction in retirement benefits.

[144]Paul Pillar, "Leaks and an Irresponsible Press," The National Interest Web site, December 26, 2013, accessed March 1, 2015, http://nationalinterest.org/blog/paul-pillar/leaks-irresponsible-press-9633.

Regardless of the reason for the leak or the government's response to the leak, this chapter illustrates the importance of preventing the unauthorized disclosure of classified information. As indicated in the introduction, media leaks have historically caused more damage to national security than spies. While this chapter presents a straightforward analysis of the deterrent effect of prosecuting individuals for disclosing our nation's secrets without authorization, it lays the groundwork for future scholarly review of Beccaria's "four pillars" and other means to stop the leak of classified information. The simple results of this analysis reveal Beccaria's "four pillars" of law enforcement deterrence are only applicable in an ideal world and not in a country like the United States where defendants are innocent until proven guilty.

As there is no discernible deterrent effect of prosecuting media leaks under the current system, other means for stopping unauthorized disclosures must be identified. Without any single means for stopping leaks, a multi-faceted approach is required. Efforts to stop unauthorized disclosures must start with prevention. Prevention efforts must start with the background investigation conducted as part of the hiring process. Although the USIC must embrace a diverse workforce to fulfill the established mission, care must be taken to ensure only the most trustworthy of those deemed the "Best and Brightest" should be hired. Prevention efforts should include the education or re-education of every individual maintaining clearance regarding the importance of source protection. This education should include the administration and execution of legally binding documents identifying the responsibilities of maintaining a clearance and the

ramifications of divulging classified information without authorization. Moreover, the same documents should be provided to all clearance holders regardless of employer.

As a reaction to 9/11, the USIC increased the free flow of information between agencies and individuals. The resulting openness resulted in individuals having access to information without the appropriate need-to-know. The perceived increase in media leaks after 9/11 has caused some to re-think this information sharing. Although prevention is an important part of stopping the leaks, assisting with the expeditious identification of a suspect assists with the celerity of punishment. Thus, the USIC should implement a working group to develop and implement classification guidelines (including access verifications) to be used consistently by each agency. The USIC must invest the necessary resources to implement accredited technology supporting reliable and timely audit capabilities able to detect anomalous activity. In addition, this technology must have the ability to preserve any collected evidence in support of possible future prosecutions.

The United States Congress and DOJ should examine current legal proceedings for national security investigations to identify changes that may create a fairer and streamlined process for both the defense and prosecution. As illustrated by the Drake case, the current procedures for CIPA should be evaluated to determine if a judge's ruling in the CIPA hearings should be allowed to be appealed by the prosecution rather than by the Attorney General. In addition, the United States Congress and DOJ should evaluate whether judges presiding over national security cases should be randomly selected from a

pool of judges with national security experience. Although they may seem superficial or slanted in favor the prosecution, experienced judges and a streamlined CIPA process favor an expeditious and fair outcome for national security cases.

Although most of the recommendations involve increasing prevention or identification capabilities, the United States Congress must do their part to eliminate leaks of classified information. As previously indicated, current espionage statutes were written in 1917 and 1949. Congress and the oversight committees should consider debating their applicability to the prosecution of media leaks especially a high-tech world with a twenty-four hour news cycle whereas anyone with internet access can be considered a journalist.

CONCLUSION

The foundation of this portfolio lies in the democratic dilemma, which involves the balancing act between security and liberty in democratic nations. The inherent distrust of the government by the inhabitants of democracies results in oversight of the government's bureaucracies. Although secrecy is a necessary condition of the intelligence services' work, intelligence services in democracies must execute their authorities while operating within the rule of law and under the watchful eye of oversight bodies. As we have learned, intelligence failures and violations of civil liberties are inevitable. Effective oversight decreases the likelihood of these occurrences and mitigates the extent of violations through constant monitoring.

This portfolio began investigating Peter Gill's theory which tied public trust to levels of security and intelligence oversight. According to Gill, the inherent distrust of the government in democracies resulted in increased intelligence, whereas the increased trust in authoritarian regimes resulted in decreased levels of intelligence oversight. This portfolio tested the applicability of Gill's theory to intelligence oversight in the United Kingdom, the United States, Canada, and Australia, which are considered similar western democratic and economically advanced nations. The research conducted for this project identified strong oversight in all of the countries. However, the applicability of Gill's theory to similar countries was not able to be proven with the available public trust data.

Although public trust polling has been conducted in the United States for decades, international polling has been inconsistent at best. As discussed in the public trust

literature, the results are only as good as the polling pool and the data input. Another potential reason for inaccurate findings could be the use of trust in Government numbers to determine levels of oversight. The accuracy of future research regarding potential linkages could be increased with consistent international public opinion polling. In addition, polling that specifically addresses public's trust in the effectiveness of the intelligence community, as well as the public's trust in the intelligence community's respect for civil liberties and the nation's laws. Future scholarship aimed correlating public trust and intelligence oversight should also consider if the metrics used for measuring strength of intelligence oversight for this chapter was effective or could be improved in some manner.

As the country with the highest level of intelligence oversight, the second chapter evaluated the effectiveness of intelligence oversight in the United States. Assumedly, little had changed in the five years since Zegart characterized congressional oversight as ineffective and sporadic. However, the recent interest in the topic provided more than enough justification for the updated and expansive review. Zegart's innovative approach to evaluating intelligence oversight using legislative activity metrics formed the foundation for the research in this portfolio. As with Zegart's research, my work found intelligence oversight in the United States to be ineffective in comparison to other oversight committees and linked this to a lack of constituent interest.

Critics of this methodology used for this portfolio argue that the oversight effectiveness cannot be solely measured merely by the number of hearings or reports

published.[145] Additionally, publication of documentation of regarding legislative activity and other oversight activities (briefings, interviews, etc.) for HPSCI and SSCI are inconsistent and at times non-existent. More important than the number of hearings or reports, is what transpires in the hearings or meetings or the content of the reports. In addition to the hearings themselves, it is important to consider the congressional response to hearings. I acknowledge the limitations of this type of metric-based analysis of intelligence oversight; however, these metrics provide a baseline for comparison between oversight committees and a general characterization of intelligence oversight.

As we have seen, the ineffectiveness of intelligence oversight can be tied to a lack of public interest. It is unclear if this lack of interest can be tied to being uninformed about intelligence, or simply feeling as if they are unaffected by intelligence. As the research has shown, it is impossible to know or even estimate the number of every ad hoc meetings or briefings, or communications amongst the oversight apparatus that occurs outside the normal course of business[146] and thus, evaluating congressional oversight is limited to the publically available and documented information. Thus, HPSCI and SSCI must improve their focus on transparency to include increased public hearings, as well as increase the tracking and publication of committee activities associated with their oversight duties. Beyond holding the USIC accountable, transparency in oversight activities can help educate the public and spur public debate on intelligence which had been lacking before the Snowden disclosures.

---

[145]Kenneth Anderson, October 17, 2011, book review of *Eyes on Spies: Congress and the United States Intelligence Community* by Amy B. Zegart, Lawfare Blog, October 17, 2011, http://new.lawfareblog.com/eyes-spies-amy-b-zegart.

[146] As evident from the inability to gauge HPSCI's legislative activity levels.

Linkages between the ineffectiveness of congressional oversight have been tied to a lack of public interest. Zegart relied on a lack of intelligence related lobbying and public affairs groups, while I relied on national election exit polling. All signs points to a lack of public interest, which correlates to a lack of congressional attention to oversight. Recent national election exit polls appear to illustrate the relative unimportance of intelligence or civil liberties to voters. However, it is important to note that neither was available to respondents as potential choices. Polling organizations should consider either expanding the potential voter issue pool, or allowing voters to reply to polling questions with their own answers.

The chapter on intelligence oversight was founded on the understanding that structural reform of congressional oversight was highly unlikely. The chances of either consolidating appropriations authority within HPSCI and SSCI were unlikely, as were considerations for the formation of a joint standing committee. Thus, the chapter focused on identifying real changes aimed at increasing the effectiveness of intelligence oversight that could occur in short order. Overwhelmingly, this chapter identified staffing levels, competency, and turnover of committee staff was as an area to be improved upon immediately. Congress should focus on increasing committee staff levels and capabilities, as well as increasing staff retention rates for HPSCI and SSCI. As the Sunlight Foundation suggests, higher salaries or other monetary compensation provides the easiest means to increase and retain committee staff. Therefore, future research of intelligence oversight should focus on USIC committee staffing issues.

In addition to Zegart's metric-based analysis, intelligence oversight literature cited the inability to pass Intelligence Authorization legislation between FY 2006-2009, the DOJ's use of the Espionage Act of 1917 to investigate and prosecute leakers, and their inability to pass vital intelligence reforms as evidence of ineptitude.[147] Of these, the prosecution of media leaks provided the most testable option based on critics claims that the draconian use of outdated laws deter potential whistleblowers and stifle free speech. The purpose of criminal prosecution is two-fold: punish the offender and deter would-be criminals. Since both sides appeared to agree on the perception of deterrence, this portfolio reviewed the case particulars for historical prosecutions of media leaks to determine if they serve as a deterrent.

The results overwhelmingly suggest that prosecuting media leaks do not serve as a deterrent to would be criminals. Critics of media leak prosecutions have claimed potential leakers would be deterred long before the disclosures of Bradley Manning and Snowden. Their disclosures, which are considered the most massive in history, along with the data presented in this chapter confirm the lack of deterrent effect. The lack of a deterrent effect combined with the negative perception of using 18 U.S. Code § 793 to prosecute media leaks should serve as an impetus for congressional consideration and potential introduction of legislation. The findings of this chapter are relevant to the topic of oversight based on the common misperception that its sole purpose is the prevention of

[147]Jennifer Kibbe, "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?," Intelligence and National Security25:1 (2010):26, accessed May 1, 2015, doi:10.1080/02684521003588104.

intelligence failures and government abuses. However, oversight includes the drafting and consideration of laws under which the USIC operates.

As the evidence has shown, DOJ will continue to prosecute individuals accused of the unauthorized disclosure of classified information to the media will continue as long as a subject can be identified, the victim agency is willing to consider releasing additional classified information during trial, and sufficient evidence is identified. Based on the ineffectiveness of intelligence oversight confirmed through this portfolio, passage of newer laws or sanctions which separate media leaks from spy cases is unlikely. Opinions of potential appropriate sanctions for media disclosures are split between criminal and administrative sanctions and fines. Future scholarship and discussion about media disclosures should include focus on identifying sanctions that punish and deter.

As there is no discernible deterrent effect of prosecuting media leaks under the current system, other means for stopping unauthorized disclosures must be identified. Without any single means for stopping leaks, a multi-faceted approach is required. Efforts to stop unauthorized disclosures must start with prevention. Prevention efforts must start with the background investigation conducted as part of the hiring process, as well as include the re-education of every individual maintaining clearance. This education should include the administration and execution of legally binding documents identifying the responsibilities of maintaining a clearance and the ramifications of divulging classified information without authorization. Moreover, the same documents should be provided to all clearance holders regardless of employer.

As a reaction to 9/11, the USIC increased the free flow of information between agencies and individuals. The resulting openness resulted in individuals having access to information without the appropriate need-to-know. The perceived increase in media leaks after 9/11 has caused some to re-think this information sharing. Although prevention is an important part of stopping the leaks, assisting with the expeditious identification of a suspect assists with the celerity of punishment. Thus, the USIC should implement a working group to develop and implement classification guidelines (including access verifications) to be used consistently by each agency. The USIC must invest the necessary resources to implement accredited technology supporting reliable and timely audit capabilities able to detect anomalous activity. In addition, this technology must have the ability to preserve any collected evidence in support of possible future prosecutions.

Although considered ineffective, intelligence oversight in the United States is the strongest of those reviewed. This strength combined with the plethora of scholarly work on the topic clearly illustrates the importance of intelligence oversight in our democracy. As long as we continue the debate about intelligence and civil liberties, the attention will the oversight committees to implement the changes necessary to increase their effectiveness and minimize the threat of intelligence failure and abuse of civil liberties.

BIBLIOGRAPHY

Activities, Select Committee to Study Governmental Operations with respect to Intelligence. "Intelligence Activities and the Rights of Americans." April 23, 1976. Accessed August 1, 2012. http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIb.htm.

Aftergood, Stephen. *USA v. Jeffrey Alexander Sterling: Selected Case Files.* May 15, 2015. http://fas.org/sgp/jud/sterling/.

Aftergood, Steven. *Selected Judicial Branch Documents on Secrecy, Leaks, Intelligence and freedom of Information.* June 5, 2014. http://fas.org/sgp/jud/ (accessed May 1, 2015).

Agency, Central Intelligence. *Australia-Oceania :: Australia* . July 10, 2012. Accessed July 29, 2012. https://www.cia.gov/library/publications/the-world-factbook/geos/as.html.

Agency, The Central Intelligence. *North America :: Canada.* 2012. Accessed August 1, 2012. https://www.cia.gov/library/publications/the-world-factbook/geos/ca.html.

Anderson, Kenneth. "Book Review: Eyes on Spies by Amy Zegart." *Lawfare Web Site.* October 2011. http://lawfareblog.com/2011/10/eyes-on-spies/3563/ (accessed May 1, 2015).

Andrew, Christopher. *The Inter-War Years.* 2012. Accessed July 29, 2012. https://www.mi5.gov.uk/home/mi5-history/mi5-between-the-wars/the-inter-war-years.html.

Apuzzo, Matt. "Times Reporter Will Not Be Called to Testify in Leak Case." *New York Times*, January 12, 2015.

Art, Robert J. "Bureaucratic Politics and American Foreign Policy: A Critique." *Policy Sciences* (Springer) 4, no. 4 (December 1973): 467-490.

Bailey, William C. "Murder, Capital Punishment, and Television: Execution Publicity and Homicide." *American Sociological Review* Vol. 55 (Oct., 1990): 628-633. Accessed on July 1, 2011. http://www.jstor.org/stable/2095860.

Bailey, William C. "Deterrence and the Celerity of the Death Penalty: A Neglected Question in Deterrence Research." *Social Forces* Vol. 58, No. 4 (June, 1980): 1308-1333. Accessed on July 1, 2011. http://www.jstor.org/stable/2577328.

Barbeau, Janet. "Evidence and Property Control." *Law & Order* Vol. 51, No.8 (Aug 2003): 96-99. Accessed August 21, 2011. http://search.proquest.com/docview/197229977/fulltextPDF?accountid=11752.

Batvinis, Raymond J. *The Origins of FBI Counterintelligence.* Lawrence: University of Kansas Press, 2007.

Becker, Gary S. "Crime and Punishment: An Economic Approach." *Journal of Political Economy (*1968): 169-217.

Betts, Richard K. "Analysis, War, and Decision: Why Intelligence Failures Are inevitable." *World Politics*, January 1978: 61-89.

Bryjak, George J, and Harold J Grasmick. "The Deterrent Effect of Perceived Severity of Punishment." *Social Forces* (1980): 471-491. Accessed on July 14, 2011. http://www.jstor.org/stable/2578032.

Burch, James. "A Domestic Intelligence Agency for the United States? A Comparative Analysis of DOmestic Intelligence Agencies and Their Implications for Homeland Security." *Homeland Security Affairs*, June 2007: 1-20.

Capitano, Joseph. "John Kiriakou Complaint - US Department of Justice." *US Department of Justice Web site.* January 19, 2012. http://www.justice.gov/sites/default/files/opa/legacy/2012/01/23/kiriakou-complaint.pdf. (accessed March 1, 2015).

Center for Responsive Politics: Lobbying Database. March 13, 2015. http://www.opensecrets.org/lobby/ (accessed May 1, 2015).

Center, Pew Research, Lee Rainee, and Mary Madden. *Americans' Privacy Strategies Post-Snowden.* March 16, 2015. http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/ (accessed March 16, 2015).

Central Intelligence Agency. "A Look Back … The National Security Act of 1947." *Central Intelligence Agency.* April 30, 2013. https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/national-security-act-of-1947.html (accessed March 1, 2015).

Clifford, J. Garry. "Bureacratic Politics." *The Journal of American History* Vol. 77, No. 1 (Jun., 1990):161-168. Accessed August 21, 2011. http://www.jstor.org/stable/2078648.

Cornell Law School. "18 U.S. Code § 793 - Gathering, transmitting or losing defense information." *Cornell Law School Web site.* https://www.law.cornell.edu/uscode/text/18/793 (accessed May 1, 2015).

Dempsey, Jim. "Domestic Intelligence Agencies: The Mixed Record of the UK's MI5." *Center for Democracy and Technology*, January 2003: 1-7.

Department, U.S. State. *A-Z List of Country and Other Area Pages.* n.d. Accessed April 15, 2013. http://www.state.gov/misc/list/index.htm.

Dillon, Robin L., Genevieve Lester, Richard S. John, and Catherine H. Tinsley. "Differentiating Conflicts in Beliefs Versus Value Tradeoffs in the Domestic Intelligence Policy Debate." *Risk Analysis*, January 1, 2011: 713-728.

Donovan, Todd, David Denemark, and Shaun Bowler. "Trust in Government: The United States in Comparative Perspective." *Western Washington University.* Accessed March 30, 2013. http://faculty.wwu.edu/donovat/trust.pdf.

Dorwart, Jeffery M. *Conflict of Duty: The U.S. Navy's Intelligence Dilemma, 1919-1945.* Annapolis: Naval Institute Press, 1983.

Dorwart, Jeffrey M. *The Office of Naval Intelligence: The Birth of America's First Intelligence Agency, 1865-1918.* Annapolis: Naval Institute Press, 1979.

Drutman, Lee. *Turnover in the House: Who keeps - and who loses - the most staff.* February 6, 2012. http://sunlightfoundation.com/blog/2012/02/06/turnover-in-the-house/ (accessed May 1, 2015).

Edelman Berland. *Edelman Trust Barometer Archive.* 2015. http://www.edelman.com/insights/intellectual-property/edelman-trust-barometer-archive/ (accessed May 1, 2015).

Federal Bureau of Investigation: Baltimore Division. "Former FBI Contract Linguist Sentenced for Leaking Classified Information to Blogger." Accessed July 21, 2011. http://www.fbi.gov/baltimore/press-releases/2010/ba052410.htm.

Federation of American Scientists. "Project on Secrecy." Accessed July 21, 2011. http://www.fas.org/sgp/jud/drake/061011-dismiss.pdf.

Gallup. *Gallup.* Accessed February 1, 2013. http://www.gallup.com/poll/5392/trust-government.aspx.

Gallup. *Congress and the Public.* http://www.gallup.com/poll/1600/congress-public.aspx (accessed March 13, 2015).

Gorman, Siobhan, and Jennifer Valentino-DeVries. "New Details Show Broader NSA Surveillance Reach: Programs Cover 75% of Nation's Traffic, Can Snare Emails." *Wall Street Journal.* August 13, 2013. http://www.wsj.com/articles/SB10001424127887324108204579022874091732470 (accessed March 1, 2015).

Gerber, Rudolph, and John Johnson. *The Top Ten Death Penalty Myths: The Politics of Crime Control.* Westport: Prager Publishers, 2007.

Gill, Peter. *Policing Politics: Security Intelligence in the Liberal Democratic State.* New York: Frank Cass & Co. LTD, 1994.

Gill, Peter. "Theories of intellligence: Where are we, where should we go and how might we proceed?" In *Intelligence Theory: Key questions and debates*, by Peter Gill, Stephen Marrin and Mark Phythian, 208-223. New York: Routledge , 2009.

Glees, Anthony, Philip H.J. Davies, and John N.L. Morrison. *The Open Side of Secrecy: Britain's Intelligence and Security Committee.* London: The Social Affairs Unit, 2006.

Gordon, Josh, and Mark Forbes. *ASIO chief concedes Bali failure.* June 20, 2003. Accessed August 1, 2012. http://www.theage.com.au/articles/2003/06/19/1055828435449.html.

Government, Australian. *About ASIO.* 2012. Accessed August 1, 2012. http://www.asio.gov.au/About-ASIO/Overview.html.

"Gov. Riley Awards Grant for More Effective Dui Prosecution." *US Fed News Service, Including US State News,* Nov 03, 2006. Accessed August 21, 2011. http://search.proquest.com/docview/469786314?accountid=11752.

Grossman, Serge, and Michael Simon. "And Congress Shall Know the Truth: The Pressing Need for Restructuring COngressional Oversight of Intelligence." *Harvard Law & Policy Review*, 2008: 435-447.

Halchin, L. Elaine, and Frederick M. Kaiser. *Congressional Oversight of Intelligence: Current Structure and Alternatives.* Washington: Congressional Research Service, 2012, 1-37.

Hoekstra, Pete. *Secrets and Leaks: The Costs and Consequences for National Security.* July 29, 2005. Accessed August 8, 2011. http://www.heritage.org/research/reports/2005/07/secrets-and-leaks-the-costs-and-consequences-for-national-security.

Hulnick, Arthur S., and Joe Wippl. "FOREIGN INTELLIGENCE AND SECURITY SYSTEMS." *Boston University.* 2009. Accessed April 10, 2013. http://www.bu.edu/ir/files/2010/06/Syllabi_IR_578_Hulnick.pdf.

Intelligence, Office of the Director of National. "2012 Report on Security Clearance Determinations." *Office of the Director of National Intelligence website.* April 12, 2013. http://www.dni.gov/files/documents/2012%20Report%20on%20Security%20Clearance%20Determinations%20Final.pdf (accessed March 1, 2015).

Intelligence, Permanent Select Committee on. *REPORT OF THE JOINT INQUIRY INTO THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001.* U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, 2002.

Investigation, Federal Bureau of. *What We Investigate.* Accessed August 1, 2012. http://www.fbi.gov/about-us/investigate/what_we_investigate.

Jackson, Brian A. *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from teh Experiences of Australia, Canada, France, Germany, and the United Kingdom.* monograph, Santa Monica: RAND Corporation, 2009.

Jackson, Brian A. *The Challenge of Domestic Intelligence in a Free Society.* mongraph, Santa Monica: RAND, 2009.

Jensen, Joan M. *Army Surveillance in America, 1775-1980.* New Haven: Yale University Press, 1991.

Johnson, Loch K. "Secret Spy Agencies and a Shock Theory of Accountability." *The University of Georgia School of Public and International Affairs.* Accessed April 14, 2013. http://intl.uga.edu/Johnson%20occasional%20paper.pdf.

Jones, Bryan, and Frank Baumgartner. *Policy Agendas Project: Datasets & Codebooks.* http://www.policyagendas.org/page/datasets-codebooks (accessed May 1, 2015).

Kibbe, Jennifer. "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?" *Intelligence and National Security*, March 10 , 2010: 24-49.

Kilpatrick, Sean. "Secret CSIS committee weighs torture's role in terror tips." *The Canadian Press*, August 6, 2012.

Klein, Ezra. "Edward Snowden, Patriot." *Washington Post.* August 9, 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward-snowden-patriot/ (accessed March 1, 2015).

Lew, Jacob J. *Memorandum M-11-08.* January 3, 2011. Accessed August 21, 2011. http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-08.pdf.

Library of Congress. *All Legislation.* https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%7D (accessed February 7, 2015).

Lowell, Abbe D. *StephenKim.org.* Accessed July 20, 2011. http://www.stephenkim.org/case.html.

Lowenthal, Mark M. *Intelligence From Secrets to Policy.* Washington, DC: CQ Press, 2009.

Marimow, Ann E. "Ex-State Department adviser Stephen J. Kim sentenced to 13 months in leak case." *Washington Post*, April 2, 2014: 1.

Masse, Todd. "Domestic Intelligence in the United Kingdom: The Applicability of the MI-5 Model to the United States." *Congressional Research Service*, May 19, 2003: 1-11.

Mattingly, Phil, and Hans Nichols. "Obama Pursuing Leakers Sends Warning to Whistle-Blowers." *Bloomberg.* 10 18, 2012. http://www.bloomberg.com/news/articles/2012-10-18/obama-pursuing-leakers-sends-warning-to-whistle-blowers (accessed 03 01, 2015).

Mayhew, David. *The Electoral Connection.* New Haven: Yale University Press., 1974.

Maxwell, Sheila Royo, and M. Kevin Gray. "Deterrence: Testing the Effects of Perceived Sanction Certainty on Probation Violations." *Sociological Inquiry* Vol. 70, No. 2 (Spring, 2000): 117-136. Accessed July 7, 2011. http://onlinelibrary.wiley.com.proxy1.library.jhu.edu/doi/10.1111/j.1475-682X.2000.tb00901.x/pdf.

McCubbins, Mathew D., and Thomas Schwartz . "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms." *American Journal of Political Science*, February 1984: 165-179.

MI5: The Security Service. 2012. Accessed July 29, 2012. https://www.mi5.gov.uk/home/about-us/how-mi5-is-governed/oversight.html.

Monaco, Lisa O. "Statement of Lisa O. Monaco." *Federation of American Scientists Web site.* February 9, 2012. http://fas.org/irp/congress/2012_hr/020912monaco.pdf (accessed May 1, 2015).

Mueller III, Robert S. *United States Government Printing Office.* June 4, 2010. Accessed July 21, 2011. S:\GPO\HEARINGS\56529.TXT.

Muldoon, Thomas C. *Russian Intelligence and Security Services: An Indicator of Democratic Reform.* PhD Thesis, accessed July 28, 2912, http://www.fas.org/irp/world/russia/ADA366081.pdf, Monterrey : Naval Post Graduate School, 1999.

Neighbour, Sally. "Hidden Agendas: Our Intelligence Services." *The Monthly*, November 2010.

Nolte, William M. "Measuring Congressional Dysfunction." *International Journal of Intelligence and Counterintelligence*, 2013: 417-420.

Parliament of Australia. *House of Representatives Committees.* Accessed May 1, 2013. http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/role.htm.

—. *Parliamentary Joint Committee on Intelligence and Security: Committee activities (inquiries and reports).* Accessed May 1, 2013. http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/reports.htm.

PBS. "Unauthorized Disclosure of Classified Information '11 Questions'." Accessed June 17, 2011. http://www.pbs.org/wgbh/pages/frontline/newswar/art/leakp_large.jpg.

Pillar, Paul. "Leaks and an Irresponsible Press." *The National Interest Web site.* December 26, 2013. http://nationalinterest.org/blog/paul-pillar/leaks-irresponsible-press-9633 (accessed March 1, 2015).

Polinsky, A. Mithchell, and Steven Shavell. "The Economic Theory of Public Enforcement of Law." *Journal of Economic Literature* Vol. 38, No. 1 (Mar., 2000): 45-76. Accessed July 5, 2011. http://www.econ.boun.edu.tr/zobuz/teaching/EC352/polinsky_shavell(1).pdf.

Posner, Richard A. *Remaking Domestic Intelligence.* Palo Alto, CA: Hoover Institution Press, 2005.

Ranked Sectors. http://www.opensecrets.org/lobby/top.php?showYear=a&indexType=c (accessed May 1, 2015).

Ransom, Harry Rowe. "Congress and the Intelligence Agencies." *Proceedings of the Academy of Political Science*, 1975.

Ross, Gary. *Who Watches the Watchmen? The Conflict Between National Security and Freedom of the Press.* Washington, D.C.: National Intelligence University, 2011.

Rovner, Joshua, Austin Long, and Amy B. Zegart. "How Intelligent Is Intelligence Reform?" *International Security* Vol. 30, No. 4 (Spring, 2006): 196-208. Accessed August 19, 20115. http://www.jstor.org/stable/4137533.

Savage, Charlie. *For U.S. Inquiries on Leaks, a Difficult Road to Prosecution.* June 12, 2012. http://www.nytimes.com/2012/06/10/us/for-us-inquiries-on-leaks-a-difficult-road-to-prosecution.html?_r=0 (accessed May 1, 2015).

Shane, Scott. "Former N.S.A. official is charged in leaks case." *New York Times*, April 15, 2010.

Security and Intelligence Review Committee. "Annual Reports." *Security and Intelligence Review Committee.* October 23, 2012. Accessed May 1, 2013. http://www.sirc-csars.gc.ca/pdfs/ar_2011-2012-eng.pdf.

Senate Select Committee on Intelligence. *Committee Activities, Special Report of the Select Committee on Intelligence, January 6, 1999 to December 15, 2000* . Washington: Government Printing Office, 2001.

Senate Select Committee on Intelligence. *Report of the Select Committee on Intelligence, Covering the Period January 4, 2005 to December 8, 2006 (April 26, 2007).* Washington: U.S. Government Printing Office, 2007.

Service, Canadian Security Intelligence. *Role of CSIS.* Accessed August 1, 2012. http://www.csis-scrs.gc.ca/bts/rlfcss-eng.asp.

Service, The Security. *What We Do.* Accessed August 1, 2012. https://www.mi5.gov.uk/home/about-us/what-we-do.html.

Shane, Scott. "Former N.S.A. official is charged in leaks case." *The New York Times*, April 15, 2010.

Shulsky, Abram N., and Gary J Schmitt. *Silent Warfare: Understanding the World of Intelligence.* Third Edition. Washington, D.C.: Potomac Books, Inc., 2002.

Somin, Ilya. "Key architect of Obamacare admitted that it was passed by exploiting political ignorance." *The Washington Post*, November 11, 2014.

State, U.S. Department of. *Background Note: United Kingdom.* March 22, 2012. Accessed July 29, 2012. http://www.state.gov/r/pa/ei/bgn/3846.htm.

Sullivan, Justin. *Yahoo CEO claims she could have been jailed for defying NSA.* September 12, 2013. http://rt.com/news/yahoo-google-nsa-jail-treason-754/ (accessed May 1, 2015).

Swanson, David. *In Convicting Jeff Sterling, CIA Revealed More Than It Accused Him of Revealing.* May 11, 2015. http://www.opednews.com/articles/In-Convicting-Jeff-Sterlin-by-David-Swanson-Iraq_Jeffery-Sterling_Jeffrey-Sterling_Nuclear-150511-867.html.

The Intelligence and Security Committee. *Annual Reports.* Accessed May 1, 2013. http://isc.independent.gov.uk/committee-reports/annual-reports.

Treverton, Gregory F. *Reorganizing United States Domestic Intelligence: Assessing the Options.* Santa Monica, CA: RAND Corporation, 2008.

United States of America v. Jeffrey Alexander Sterling. 1:10-cr-00485-LMB (United States District Court for the Eastern District of Virginia, December 22, 2010).

"USA v. Jeffrey Alexander Sterling: Selected Case Files." *Federation of American Scientists website.* December 22, 2010. http://fas.org/sgp/jud/sterling/ (accessed May 15, 2015).

U.S. Department of Justice. "Criminal Resource Manual 2054 Synopsis of Classified Information Procedures Act (CIPA)." *US. Department of Justice website.*

http://www.justice.gove/usao/eousa/foia_reading_room/usam/title9/crm02054.htm (accessed March 1, 2015).

U.S. State Department. *A-Z List of Country and Other Area Pages.* 2013. Accessed April 10, 2013. http://www.state.gov/misc/list/index.htm.

Wainstein, Kenneth L. *Federation of American Scientists.* May 12, 2010. Accessed July 21, 2011. http://www.fas.org/irp/congress/2010_hr/051210wainstein.pdf.

Watch, RCMP. *Air India: How a massive intelligence failure led to 329 deaths.* June 7, 2010. Accessed August 1, 2012. http://www.rcmpwatch.com/air-india-how-a-massive-intelligence-failure-led-to-329-deaths/.

Young, Chris. "CSIS boss grilled about spying in security certificate case." *CBS News Canada.* August 1, 2012. Accessed August 5, 2012. http://www.cbc.ca/news/canada/story/2012/08/01/mohamed-mahjoub-security-certificate-hearing.html.

Zegart, Amy B. *Eyes on Spies: Congress and the United States Intelligence Community.* Stanford: Hoover Institution Press, 2011.

Zegart, Amy, and Julie Quinn. "Congressional Intelligence Oversight: The Electoral Disconnection." *Intelligence and National Security*, December 2010: 744-766.

Zegart, Amy, and Julie Quinn. "Policemen, Firefighters, and Spooks: How Oversight Varies Across Policy Domains." In *Eyes on Spies: Congress and the United States Intelligence Community*, by Amy B. Zegart, 55-84. Stanford: Hoover Institution Press, 2011.

—. *Australian Security Intelligence Organisation Act 1979* . May 10, 2011. Accessed July 29, 2012. http://www.comlaw.gov.au/Details/C2011C00364.

—. *Reviews.* October 22, 2012 . Accessed May 1, 2013. http://www.sirc-csars.gc.ca/rvwetd/index-eng.html.

—. *Committee Reports.* Accessed May 1, 2013. http://isc.independent.gov.uk/committee-reports.

—. *www.Congress.gov.* https://www.congress.gov/congressional-reports/about (accessed February 26, 2015).

—. "Unauthorized Disclosure of Classified Information." *Federation of American Scientist website.* February 9, 2012. http://fas.org/irp/congress/2012_hr/020912monaco.pdf (accessed March 15, 2015).

—. "For U.S. Inquiries on Leaks, a Difficult Road to Prosecution." *New York Times.* June 9, 2012. http://www.nytimes.com/2012/06/10/us/for-us-inquiries-on-leaks-a-difficult-road-to-prosecution.html?_r=0 (accessed March 28, 2015).

—. "Key architect of Obamacare admitted that it was passed by exploiting political ignorance." *Washington Post*, November 11, 2014.

CURRICULUM VITAE

Michael B. Homburg was born on May 18th 1976 in New Orleans, Louisiana. He has a Bachelor of Science in Marine Engineering from the United States Merchant Marine Academy. He is a Special Agent in the Federal Bureau of Investigation currently assigned to the Federal Bureau of Investigation Headquarters in Washington, DC.